Office of Inspector General | United States Postal Service

Audit Report

Integrity of the U.S. Postal Service's Social Media Presence

Report Number 20-278-R21 | May 12, 2021

Table of Contents

Highlights

Objective

Our objective was to assess the U.S. Postal Service's social media and digital channel security posture. We also assessed whether policies are in place to protect the integrity of the Postal Service's official social media and digital channel presence.

The Postal Service uses social media to promote its brand, products, and services and to create a community of customers. The Corporate Communications office is responsible for the social media program where they engage with more than 790,000 Facebook and 181,000 Twitter followers. Threat actors may take advantage of this vast audience to discredit or leverage the brand for personal gain.

To accomplish our objective, we contracted with a provider to assess the security posture of high visibility or high-risk Postal Service assets/resources on various social media platforms – such as Facebook and Twitter – and digital channels – such as recruitment sites – that make up the Postal Service's digital presence. We also reviewed Postal Service policies and spoke with personnel responsible for the official digital presence to determine compliance with policy and alignment with best practices.

Findings

We identified security threats and business risks associated with the Postal Service's social media and digital channels. We also found that policies and procedures were not adequate to protect the integrity of the Postal Service's official social media and digital channel presence.

We found that the Postal Service was not effectively monitoring for the unauthorized use of its organizational information in accordance with best practices. Specifically, we identified multiple fraudulent or deceptive websites and social media accounts purporting to be Postal Service sites, as well as Postal Service-branded goods and services for sale online without authorization. This occurred because management was only monitoring for unauthorized use of the domain name and because the process for monitoring for other intellectual property infringement was time-consuming and inefficient. Without effective monitoring capabilities, unauthorized use of organizational information could go undetected, which could result in customers being misled into thinking they are on a legitimate site, leading to reputational damage, loss of consumer trust, or potential fraud against the customer.

We also found the Corporate Information Security Office (CISO) did not follow best practices to restrict the use of work email addresses for creating accounts on external sites. Specifically, we identified 3,439 Postal Service email addresses on the dark web that were involved in known data breaches of non-Postal Service systems such as retail, gaming, and dating sites. Creating personal accounts with work email addresses increases the risk that threat actors could use this information to hijack accounts, steal data, and commit fraud.

In addition, we found social media accounts intended to officially represent the Postal Service were created without the approval required by policy. Specifically, we identified unapproved accounts for 15 post offices, nine departments, three sales teams, and multiple employees using their social media accounts in an official capacity without the proper approval. This occurred because management did not establish an automated process to proactively monitor for unapproved pages, nor did they have an effective account approval process. Further, we found the Postal Service did not follow best practices to document official social media account management procedures. Management stated they did not see a need for formal documentation because there are a limited number of users with social media responsibilities. Without sufficient social media account management processes, the Postal Service is unable to ensure consistent branding and messaging, creating a risk to the integrity of the Postal Service's digital presence.

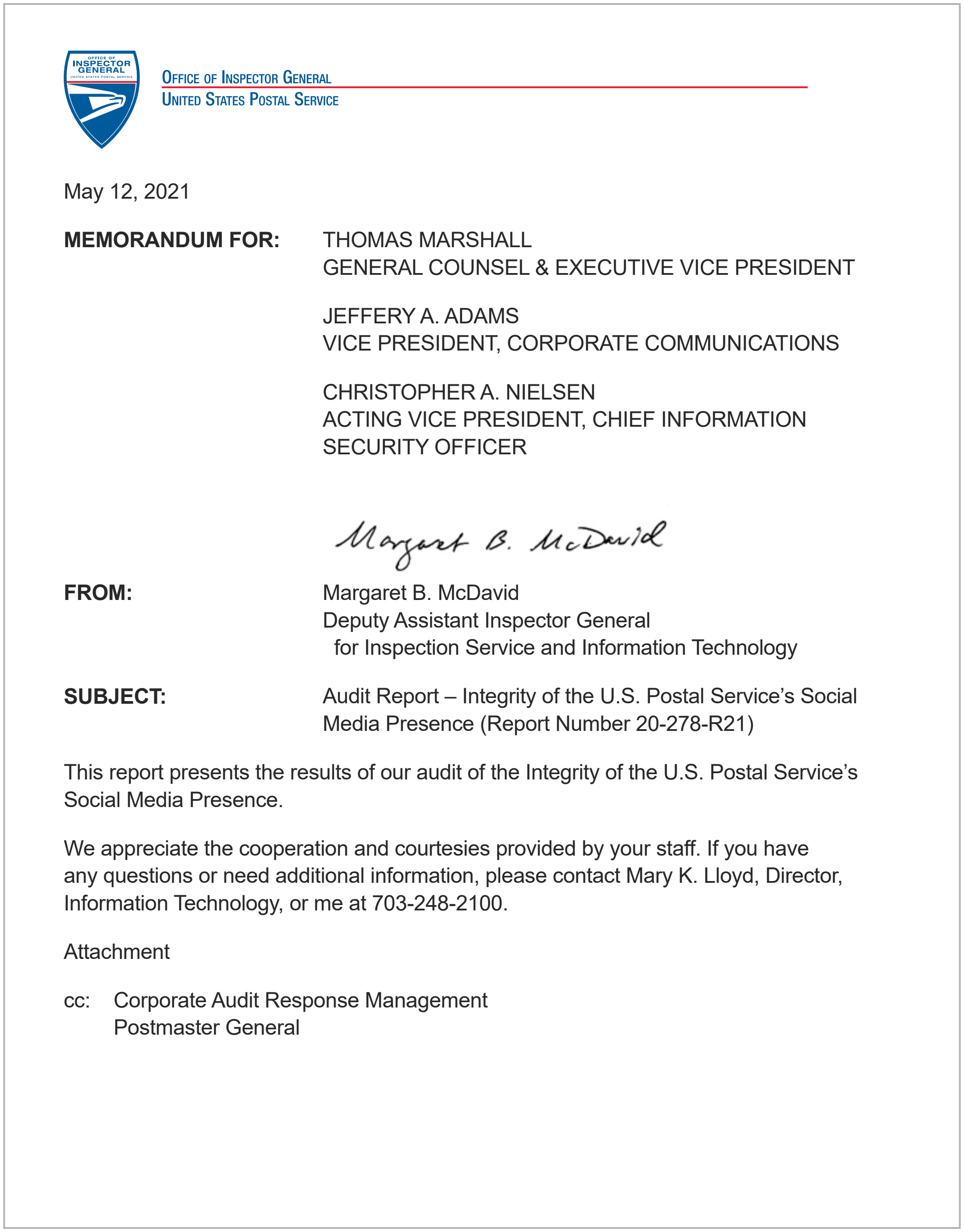
Finally, we found that management did not define or document organizational roles and responsibilities for responding to threats to the Postal Service's digital presence in accordance with best practices. Depending on the situation, the Law Department, Inspection Service, CISO, Public Relations, Corporate Communications, or Human Resources may need to be involved in response activities. Management stated they are in regular communication with each other and see no need for a formally documented plan. Without clearly defined roles, the Postal Service may not be able to respond to threats to its brand in a timely manner, which could cause reputational damage.

Recommendations

We recommend management:

1. Establish a permanent automated monitoring solution of publicly available digital information to identify and address unauthorized use of organizational information.
2. Update internal information security policy to include restrictions on the use of work email addresses on external sites.
3. Establish an effective social media account approval process and document social media account management procedures.
4. Develop a process to inform employees of the social media account establishment policy.
5. Establish an automated process to monitor social media to identify and address unapproved pages and accounts created to represent the Postal Service.
6. Identify appropriate stakeholders and develop a formal plan with roles and responsibilities for identifying and responding to fraudulent activity on social media and digital channels.

Transmittal Letter



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

May 12, 2021

MEMORANDUM FOR: THOMAS MARSHALL
GENERAL COUNSEL & EXECUTIVE VICE PRESIDENT

JEFFERY A. ADAMS
VICE PRESIDENT, CORPORATE COMMUNICATIONS

CHRISTOPHER A. NIELSEN
ACTING VICE PRESIDENT, CHIEF INFORMATION SECURITY OFFICER

Margaret B. McDavid

FROM: Margaret B. McDavid
Deputy Assistant Inspector General
for Inspection Service and Information Technology

SUBJECT: Audit Report – Integrity of the U.S. Postal Service's Social Media Presence (Report Number 20-278-R21)

This report presents the results of our audit of the Integrity of the U.S. Postal Service's Social Media Presence.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Mary K. Lloyd, Director, Information Technology, 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 Integrity of the U.S. Postal Service's Social Media Presence (Project Number 20-278). Our objective was to assess the Postal Service's social media and digital channel security posture. We also assessed whether policies were in place to protect the integrity of the Postal Service's official social media and digital channel presence. Social media and digital channels include business communication platforms such as Facebook, LinkedIn, Twitter, forums, domains, mobile app stores, and recruitment sites. Together, these make up the Postal Service's digital presence. In addition, an organization's security posture refers to its overall cybersecurity strength and how well it can predict, prevent, and respond to everchanging cyberthreats. See Appendix A for additional information about this audit.

Background

Modern organizations increasingly rely on digital channels to engage customers, interact with employees, and grow business; the Postal Service is no exception. The Postal Service uses social media to promote its brand, products, and services; to create a community of customers and fans; and to further its mission of providing efficient, reliable, and universal postal products and services.

In 2019, nearly 220 million Americans used social networks at least once a month[1] and analysis reveals a surge of use amid the 2020 Coronavirus pandemic.[2] In April 2020, 47 percent of internet users reported spending more time on social media. It is estimated the number of social media users will increase by more than 20 million in the U.S. alone by 2025.[3]

The Corporate Communications office is responsible for the Postal Service's social media program and engages with over 790,000 Facebook and 181,000 Twitter followers. They also use LinkedIn, YouTube, Pinterest, Instagram, and the Postal Posts Blog[4] to connect with employees and customers. Created in 2015, the Social Media Department staff has grown from four to nearly 30 employees. Roles include an editorial staff, social media customer response associates, and a social listening team whose focus is business intelligence, or what people are saying about the USPS.

> *"The Corporate Communications office is responsible for the Postal Service's social media program and engages with over 790,000 Facebook and 181,000 Twitter followers."*

The Postal Service has a policy[5] in place to govern the use of social media by its employees and contractors when serving in an official or professional capacity. An official account is any social media account, site, or presence that was established to represent the Postal Service. Examples include the Postal Service's official Facebook and Twitter pages. Policy states that the social media team must approve official accounts. Additionally, management permits individual employees to have social media accounts for the purpose of performing their job responsibilities. Examples include LinkedIn and Twitter accounts for sales or other business purposes. According to policy, these individuals must obtain authorization from the social media team before posting content. Further, policy stipulates that the social media management team runs the day-to-day operations of the social media function.

The ASM[6] also governs the use of Postal Service trademarks and copyrighted materials. The Law Department is responsible for licensing matters, intellectual property[7] enforcement, and a variety of other issues. Intellectual property enforcement includes issuing cease and desist letters to individuals or entities

[1] Statista.com article, *Social Media Usage in the United States - Statistics & Facts*, May 19, 2020.
[2] Digital Information World, *Analysis Reveals a Surge in Digital Activity and Social Media Growth Amid Coronavirus Pandemic*, dated April 27, 2020.
[3] Statista.com article, *Social Media Usage in the United States - Statistics & Facts*, May 19, 2020.
[4] Allows the public to learn about products, services, technological innovations, history, customers, and employees (https://uspsblog.com).
[5] *Administrative Support Manual,* Section 363, Social Media Policy, updated through July 31, 2020.
[6] ASM Section 663, Rights and Permissions, dated December 2020.
[7] Products the law protects from use by others such as patents, copyrights, trademarks, and trade secrets.

> *"We identified multiple fraudulent or deceptive websites and social media accounts purporting to be the Postal Service."*

impersonating the Postal Service by using the name and logo on social media and digital channels. Intellectual property enforcement may also include sending a referral to law enforcement if it warrants legal action beyond a cease and desist order.

Social media platforms have their own acceptable use policies and expect users to abide by published standards of behavior. For instance, Twitter prohibits impersonation accounts that "pose as another person, brand, or organization in a confusing or deceptive manner." According to the Twitter Transparency Center,[8] more than 120,000 accounts were suspended for violating impersonation rules between January - June 2020.

Fraudulent activity on social media and digital channels can have a devastating impact, leading to distrust, damaged reputations, and financial loss. While there may be legal consequences for impersonating someone on social media, the identity of the threat actor would have to be discovered, which is often not easy. Threat actors may take advantage of large social media audiences and use various means to launch scams or attacks through digital channels. For example, they may acquire usernames and passwords from a data breach[9] or password dump site[10] on the dark web[11] for malicious purposes such as stealing data from an organization's systems. They may also create fraudulent mobile applications or initiate phishing campaigns[12] to mislead victims into downloading malware[13] or revealing sensitive personal information. In addition, threat actors can create fake social media accounts to masquerade as credible brands or company executives, then post derogatory content or fake updates about the brand they appear to be representing.

Finding Summary

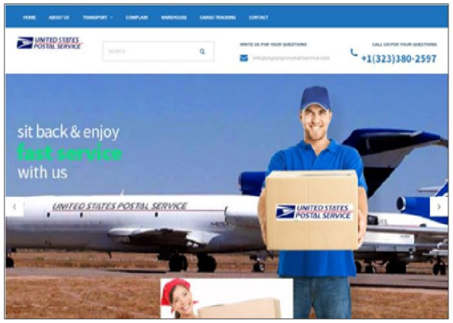
We identified security threats and business risks associated with the Postal Service's social media and digital channels. We also found that policies and procedures were not adequate to protect the integrity of the Postal Service's official social media and digital channel presence.

Finding #1: Use of Organizational Information

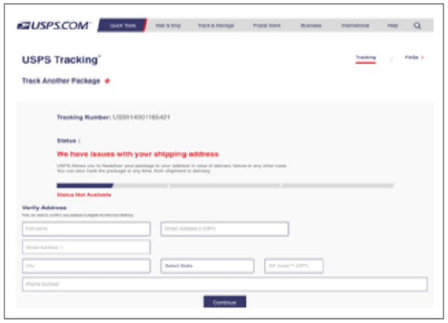
The Postal Service did not effectively monitor for the unauthorized use of its organizational information in accordance with best practices.[14] Specifically, we identified multiple fraudulent or deceptive websites and social media accounts purporting to be the Postal Service, as well as unauthorized online sales of Postal Service-branded goods and services. For example, we found:

- Perpetrators using the USPS name or logo to impersonate the Postal Service or set up phishing sites (see Figure 1).

Figure 1. Example of Two Fraudulent Websites


HOME
ABOUT US
TRANSPORT
COMPLAIN
WAREHOUSE
CARGO TRACKING
CONTACT
UNITED STATES POSTAL SERVICE
SEARCH
WRITE US FOR YOUR QUESTIONS
CALL US FOR YOUR QUESTIONS
+1(323)380-2597
sit back & enjoy
fast service
with us
UNITED STATES POSTAL SERVICE
UNITED STATES POSTAL SERVICE

Source: https://uspsexpressmailservice.com/

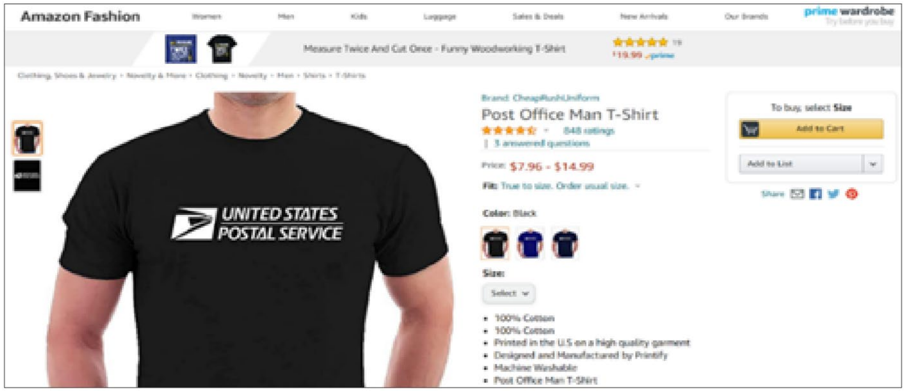


Source: https://boroskop.net/usaa/

[8] Includes sections covering information requests, removal requests, copyright notices, trademark notices, email security, Twitter rules enforcement, platform manipulation, and state-backed information operations.
[9] A security incident in which information is accessed without authorization.
[10] A location where a compromised website's contents are dumped on the web, typically exposing the usernames and the passwords of the people who visit the site.
[11] Websites that use the public internet but require specific software for access. It is not indexed by search engines to ensure anonymity.
[12] A cybercrime in which scammers try to lure sensitive information or data from you by disguising themselves as a trustworthy source. Phishers use multiple platforms.
[13] An abbreviation of "malicious software." This is software that is specifically designed to gain access to or damage a computer, usually without the knowledge of the owner.
[14] *NIST Special Publication 800-53, Revision 5*, dated September 2020. This publication is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems.

- Unauthorized third parties selling products with the Postal Service logo such as shipping labels, apparel, and other goods on social media and e-commerce marketplaces such as Amazon, eBay, and Etsy (see Figure 2).

Figure 2. Example of Unauthorized Sale of Product with Logo



Measure Twice And Cut Once - Funny Woodworking T-Shirt
$19.99 prime

Clothing, Shoes & Jewelry › Novelty & More › Clothing › Novelty › Men › Shirts › T-Shirts

Brand: CheapRushUniform
Post Office Man T-Shirt
848 ratings
3 answered questions

Price: $7.96 - $14.99
Fit: True to size. Order usual size.

Color: Black

Size: Select

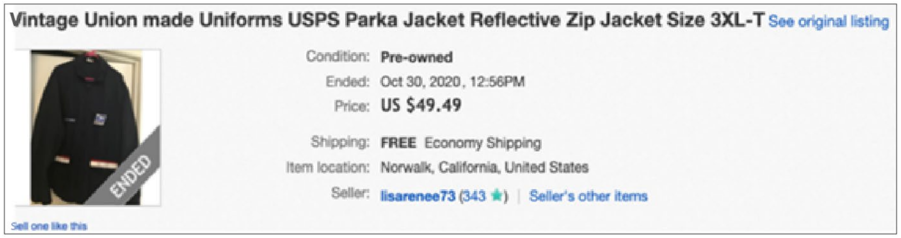
To buy, select Size

- 100% Cotton
- 100% Cotton
- Printed in the U.S on a high quality garment
- Designed and Manufactured by Printify
- Machine Washable
- Post Office Man T-Shirt

Source: https://www.amazon.com/CheapRushUniform-Post-Office-Man-T-Shirt/dp/B078Z2HNGL

- Postal Service uniforms for sale on eBay (see Figure 3).

Figure 3. Example of Unauthorized Uniform Sale



Vintage Union made Uniforms USPS Parka Jacket Reflective Zip Jacket Size 3XL-T

Condition: Pre-owned
Ended: Oct 30, 2020, 12:56PM
Price: US $49.49
Shipping: FREE Economy Shipping
Item location: Norwalk, California, United States
Seller: lisarenee73 (343)

Source: https://www.ebay.com/itm/Vintage-Union-made-Uniforms-USPS-Parka-Jacket-Reflective-Zip-Jacket-Size-3XL-T-/353250056095

We also identified a Twitter account impersonating a high-ranking Postal Service official, which we immediately brought to management's attention. They took corrective action to have Twitter suspend the account; therefore, we are not making a specific recommendation on this issue.

The Procurement and Property Law Department was only actively monitoring for the unauthorized use of "Postal" and "USPS" in the domain name. They stated that intellectual property infringement matters were being brought to their attention more frequently than in the past and that manual review and cease and desist actions are time consuming and inefficient processes. Therefore, on September 15, 2020, the Postal Service initiated a six-month trial for brand protection services. In response to fraudulent activity identified in the trial, the Postal Service stated over 2,500 items were removed from marketplaces and more than 300 social media takedown requests were initiated. However, the Postal Service has not signed a contract for a permanent monitoring solution.

Without effective monitoring capabilities, unauthorized use of organizational information could go undetected, which could result in customers being misled into thinking they are on a legitimate site. For example, a misled customer might inadvertently reveal sensitive personal information or rely on false information, which could lead to reputational damage, loss of consumer trust, or potential fraud committed against the customer. In addition, the public places an inherent trust in the Postal Service uniform and selling those uniforms online to someone with malicious intent can create a risk to public safety.

> *"Without effective monitoring capabilities, unauthorized use of organizational information could go undetected, which could result in customers being misled into thinking they are on a legitimate site."*

Recommendation #1

We recommend the **General Counsel & Executive Vice President** establish a permanent automated monitoring solution of publicly available digital information to identify and address unauthorized use of organizational information.

Finding #2: Use of Work Email Addresses

The Corporate Information Security Office (CISO) did not restrict the use of work email addresses for creating accounts on external sites in accordance with best practices.[15] We found 3,439 unique Postal Service email addresses associated with 61 known data breaches (see Appendix B) of non-Postal Service systems disclosed on the dark web. Some of these data breaches were associated with retail, gaming, and dating sites, where employees created accounts using their work email address and possibly their work password. According to a 2019 online security survey by Google, 65 percent[16] of people use the same password for multiple or all accounts. Our assessment initially included 40 employees; however, because 78 percent of the in-scope employees were involved in a breach, we expanded our search to include the entire usps.gov email domain. Specifically, we found the following:

- Of the 40 in-scope employees, 31 were involved in at least one breach.
- There were 3,408 additional Postal Service email addresses involved in at least one breach.

Postal Service policy[17] summarizes the appropriate use and protection of Postal Service resources; however, the CISO did not include restrictions on the use of work email addresses on external sites. Management agreed that they need to make users aware of the risks. Although there may be a need to create business accounts on external sites, creating personal accounts with work email addresses increases the risk that threat actors could use this information to hijack accounts, steal data, and commit fraud.

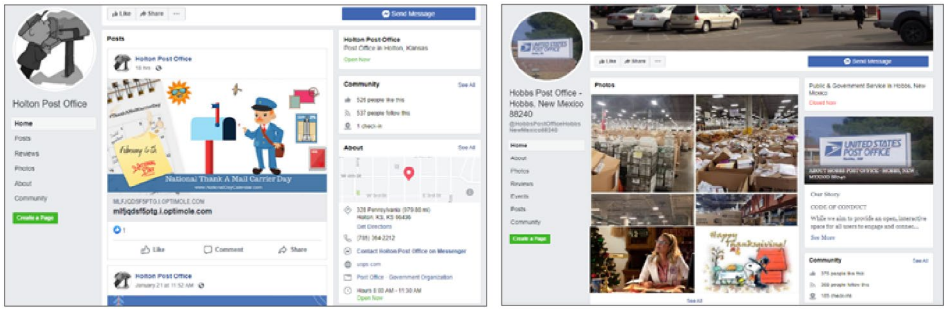
Recommendation #2

We recommend the **Vice President, Corporate Information Security Office**, update Handbook AS-805-C, *Information Security Requirements for All Personnel*, to include restrictions on the use of work email addresses on external sites.

Finding #3: Social Media Account Management

Social media accounts intended to officially represent the Postal Service were created without the approval required by policy.[18] For example, we found unapproved accounts for 15 post offices, nine departments, three sales teams, and multiple employees using their social media accounts in an official capacity without the proper approval. See Figure 4 for examples of the unapproved Holton, KS, and Hobbs, NM, post office social media pages. The Director, Digital Communications, confirmed that post offices are not approved to establish a digital presence because it becomes increasingly difficult to manage and ensure consistent branding and messaging. During our audit, management took corrective action by instructing the post offices to deactivate the accounts.

Figure 4. Example of Two Unapproved Post Office Pages


Holton Post Office
Send Message
National Thank A Mail Carrier Day
Hobbs Post Office - Hobbs, New Mexico 88240
UNITED STATES POST OFFICE
Happy Thanksgiving!

Source: https://www.facebook.com/Holton-Post-Office-496906437322014/

Source: https://www.facebook.com/HobbsPostOfficeHobbs NewMexico88240/

These accounts went undetected because management did not establish an automated process to proactively monitor for unapproved pages, nor did they have an effective account approval process. In addition, management stated that employees were unaware of the account establishment policy because communicating the policy to a workforce of over 600,000 employees is an ongoing challenge.

[15] *NIST Special Publication 800-53*, Revision 5, dated September 2020.
[16] HelpNetSecurity article, "The Password Reuse Problem is a Ticking Time Bomb", dated November 12, 2019.
[17] Handbook AS-805-C, *Information Security Requirements for All Personnel,* dated May 2020.
[18] ASM Section 363, Social Media Policy, updated through July 31, 2020.

> *"The Postal Service may not be able to respond to threats to the digital presence in a timely manner, which could damage the Postal Service's brand or reputation."*

We also found Digital Communications did not follow best practices to document social media account management procedures. For example, they did not establish written procedures for assigning and revoking user permissions to the official Postal Service Facebook page. Further, no written procedures existed for changing the shared password for the official Twitter account when employees are transferred or terminated. Management did not see a need for formal documentation because there are a limited number of users with social media responsibilities. However, National Institute of Standards and Technology (NIST)[19] states that organizations should establish written account management procedures for revoking access and changing shared passwords when individuals are transferred or terminated.

Without sufficient social media account management processes and procedures, the Postal Service is unable to ensure consistent branding and messaging, creating a risk to the integrity of the Postal Service's digital presence.

Recommendation #3

We recommend the **Director, Digital Communications**, establish an effective social media account approval process and document social media account management procedures.

Recommendation #4

We recommend the **Vice President, Corporate Communications**, develop a process to ensure employees are informed of the social media account establishment policy.

Recommendation #5

We recommend the **Vice President, Corporate Communications**, develop a process to ensure employees are informed of the social media account establishment policy.

Finding #4: Roles and Responsibilities

We found management did not define or document organizational roles and responsibilities for responding to threats to the Postal Service's digital presence in accordance with best practices. Depending on the situation, the Law Department, Inspection Service, CISO, Public Relations, Corporate Communications, or Human Resources may need to be involved in response activities. We discussed roles and responsibilities with each of these groups and found conflicting information. For instance, when the audit team found a Twitter account impersonating a high-ranking Postal Service official, we notified the Corporate Communications office. They contacted the Law Department, which issued a takedown request to Twitter. OIG management also discussed the matter with CISO, which issued a separate takedown request directly to Twitter. In addition, an inspector with the Postal Inspection Service told us they also issue takedown requests.

Best practices recommend organizations develop a social media playbook that identifies roles and responsibilities for managing social media risks.[20] Management stated they are in regular communication with each other and see no need for formal documentation. As a result, the Postal Service may not be able to respond to threats to the digital presence in a timely manner, which could damage the Postal Service's brand or reputation.

Recommendation #6

We recommend the **Vice President, Corporate Communications**, identify the appropriate stakeholders and develop a formal plan with roles and responsibilities for identifying and responding to fraudulent activity on social media and digital channels.

[19] *NIST Special Publication 800-53*, Revision 5, dated September 2020.
[20] For example, University of Pittsburgh Clinical Translational Science Institute, *Social Media Playbook Guidelines and Best Practices*, modified December 2, 2019.

Other Matters

While conducting this audit, we identified issues that resulted in the issuance of two management alerts:

- A news article that publicly disclosed a known smishing[21] campaign targeting Postal Service customers. Perpetrators sent customers text messages about a delivery claiming to be from the Postal Service. The message included a link to attempt to steal the recipients' credentials or install malware on their device. As a result, we issued the *Active Smishing Campaign Masquerading as the U.S. Postal Service* alert (Report Number 21-018-R21, dated December 23, 2020).
- Indicators of availability issues associated with the National Change of Address[22] database and its related applications. A news article claimed the Postal Service stopped fully updating the National Change of Address system for 20 days during August 2020, affecting at least 1.8 million new change of addresses. We also found Twitter accounts citing issues with the ability to submit an address change request. As a result, we issued the *Issues Submitting and Processing Change of Address Requests* alert (Report Number 21-017-R21, dated February 2, 2021).

Management's Comments

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

Regarding finding 1, management agreed there is room to improve overall monitoring on social and other digital channels but stated that the OIG did not note that they made progress and worked with social platform providers to take down sites that were not deemed authentic.

Management partially agreed with finding 3 because it is a two-part finding. Regarding part one, they believe their communication of ASM 363, the official USPS social media policy document, has been effective because with over 644,000 employees, the OIG found fewer than 30 unapproved sites. Management agreed with part two of the finding.

Regarding recommendation 1, management agreed and stated they entered a one-year renewable contract on March 15, 2021 to continue use of the monitoring tool they implemented on a temporary basis during the period covered by the audit.

Regarding recommendation 2, management agreed and stated they will update Handbook AS-805-C by December 31, 2021.

Regarding recommendation 3, management partially agreed and stated they will modify existing policy around ownership of USPS social media platforms to reduce the risk of unauthorized use. However, management stated that the Social Media team does indeed account for people who register for legitimate social media access on USPS-approved equipment through e-Access. Further, people who request access must justify their use and acknowledge they have read ASM 363, the official USPS social media policy document. The target implementation date is December 31, 2021.

Regarding recommendation 4, management agreed there is always an opportunity to communicate more. They stated that they have sent several communications centered around the use of social media in the workplace and on a personal level to remind employees of the challenges imposed on them. Management also stated that although there are 644,000 USPS employees and the OIG found very few instances of unauthorized accounts, their goal should always be to eliminate these occurrences to protect the brand and integrity of the Postal Service as a whole. The target implementation date is July 31, 2021.

Regarding recommendation 5, management agreed and stated the Social Media team manually monitors to identify and shutdown fraudulent sites to the best of its ability given a financially challenging environment that struggles for resources. They stated that they have partnered with the Law Department as per recommendation 1, are currently in a training status, and will be fully up and running by September 30, 2021.

[21] A form of phishing in which someone tries to trick you into giving them your private information via a text message.
[22] A request to the USPS to reroute mail for all or selected individuals at the specified address.

Regarding recommendation 6, management agreed and stated they will work specifically to develop a more formalized response approach by September 30, 2021. However, they stated it is important to understand that the plan will rely on the judgment of the Social Media team to best delegate from where the response should originate. They also stated that depending on the urgency of the issue, there may be overlap in responsibilities and that the source of the initial complaint or issue must be considered.

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

Evaluation of Management's Comments

The OIG considers management's comments responsive to recommendations 1, 2, 4, 5, and 6. Action plans to address these recommendations should resolve the issues identified in this report. We consider management's comments partially responsive to recommendation 3.

Regarding finding 1, we specified in the report that the Postal Service removed 2,500 items from marketplaces and initiated more than 300 social media take down requests as identified during their six-month trial for brand protection services.

Regarding finding 3, although our limited scope only identified 30 unapproved sites, there could potentially be more because management stated that employees were unaware of the account establishment policy. Even one unapproved site could lead to inconsistent branding and messaging, creating a risk to the integrity of the Postal Service's digital presence.

Regarding recommendation 1, we reviewed the one-year renewable contract and agree to close this recommendation upon issuance of the report.

Regarding the first part of recommendation 3, we found that almost 30 percent of the users on the list of verified social media users, supplied to us by the social media team, had not requested approval through e-Access. When we brought this to management's attention, they reached out to those users and requested they submit an e-Access request. We agree with management that Section 363.3 of ASM 363, Social Media Policy, states that if a user requires access to one or more restricted social media sites on Postal Service-issued equipment for work-related purposes, they must apply through e-Access. However, Section 363.5 states that anyone using social media in an official or professional capacity must obtain prior authorization from an account administrator, authorized officer, or the Social Media Management Team. The policy does not state the method in which they are to obtain authorization. We understood that the list of verified social media users the social media team supplied to us were indeed these employees who used social media in an official or professional capacity, 30 percent of whom did not have the appropriate authorization.

Regarding the second part of recommendation 3, the action plan to modify existing policy around ownership of the USPS social media platforms should resolve the issues identified in this report. This is with an understanding that, as stated by management with respect to finding 3, this includes designing a more cohesive written instruction set from their senior social media strategist.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. Recommendations 2, 3, 4, 5, and 6 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. We consider recommendation 1 closed with the issuance of this report.

Appendices

Click on the appendix title below to navigate to the section content.

Appendix A: Additional Information

Scope and Methodology

Our audit scope included a continuous monitoring assessment from September 15, 2020 to January 15, 2021 covering the following Postal Service assets:

- The Postal Service brand
- Two Postal Service products - Informed Delivery[23] and Change of Address[24]
- Forty high visibility/high risk USPS employees
- One physical location - L'Enfant Plaza (USPS Headquarters)
- The USPS web and email domains - usps.com and usps.gov

To accomplish our objective, we contracted with a provider to identify fraudulent activity or potentially compromised data across public data sources including:

- Social networks (Facebook, Twitter, Instagram, LinkedIn, YouTube)
- Deep[25] & Dark Web
- Mobile app stores
- Human Resources & recruitment sites
- Global marketplaces

The provider granted the audit team real-time access to their platform where we analyzed 795 alerts. We obtained verified account lists from the Postal Service to determine which alerts pertained to legitimate postal sites, accounts, and pages and those which were potentially fraudulent. In addition, the audit team:

- Identified roles and personnel responsible for official social media and digital channels.
- Reviewed the social media policy for compliance and alignment with industry best practices.
- Reviewed ServiceNow[26] data to determine if there are any known issues/trends with official social media or digital channels.

We conducted this performance audit from August 2020 through May 2021 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 14, 2021 and included their comments where appropriate.

The audit team assessed the reliability of the data in the provider's platform by generating an alert report and reviewing all relevant fields to ensure completeness. We also compared the report provided by the contractor to our report to ensure the data was valid. 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 conducted within the last five years.

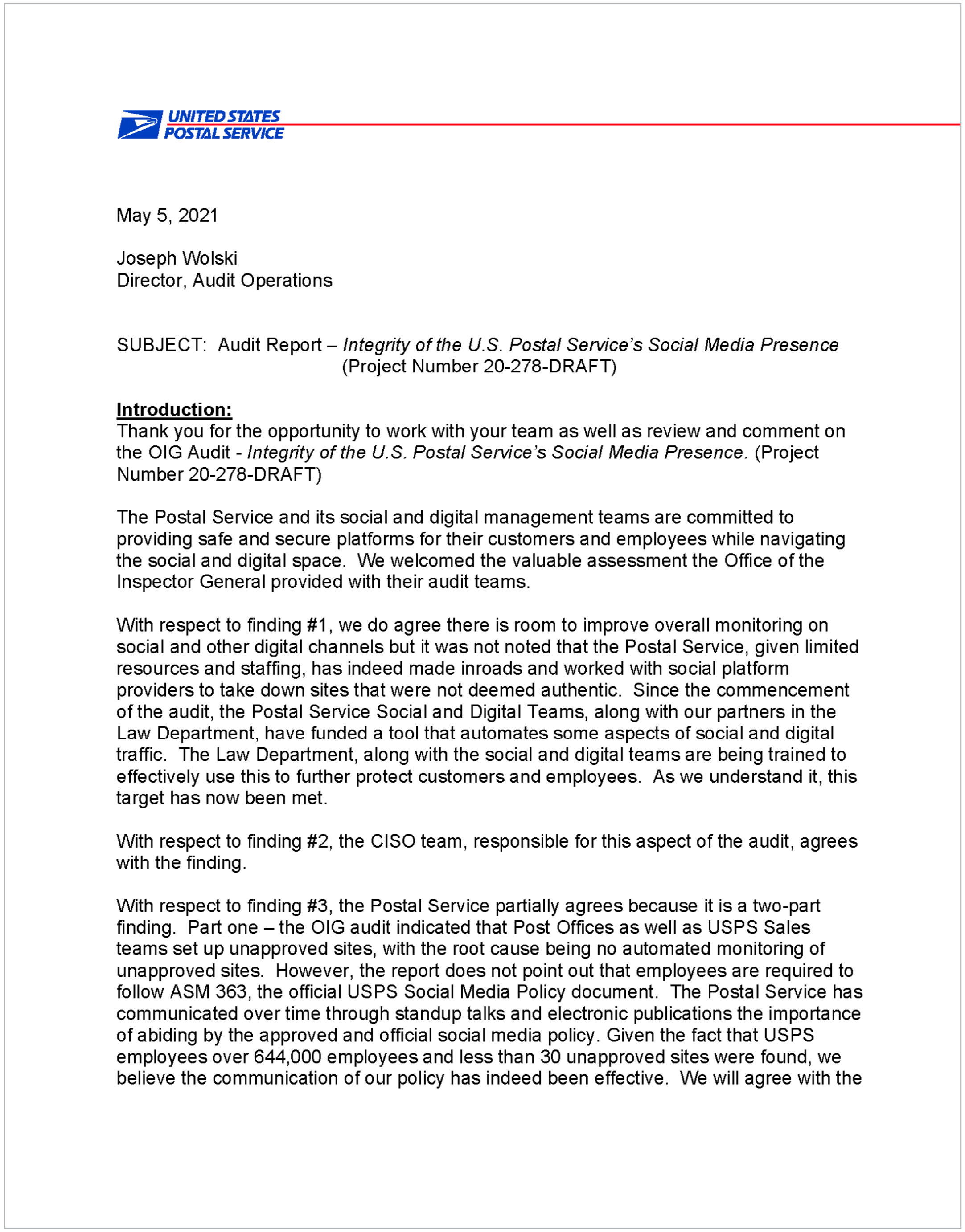
[23] A notification feature that gives residential consumers the ability to digitally preview their mail and manage package delivery.
[24] A request to the USPS to reroute your mail.
[25] Refers to information that companies, developers, and websites tell Google not to search or categorize. It does not come up in a web search; however, much of it can be accessed by typing in a direct web address.
[26] A self-help service portal where USPS users can request help or report information technology issues.

Appendix B: Data Breach Information

The table below identifies the 61 breached entities and the number of USPS email addresses associated with each.

Breached Entity	Number of Addresses
123RF (Inmagine Group)	21
Adapt	5
Animal Jam	3
AntiPublic	6
Apollo	25
Aptoide	1
B2BUSABusiness	1
Canva	1
Chatbooks	4
CitOday	705
Collection1	1
DataAnLeads	10
DB8151DD (Unknown data breach)	663
Disqus	1
Drizly	1
Evite	9
Exactis	18
Exploitin	4
Factual	14
Friend Finder	54
GeniusU	2
Glofox	3
Havenly	4
Home Chef	86
Houzz	1
KayoMoe	3
Lead Hunter	105
Linkedin	13
LiveAuctioneers	20
LiveJournal	6
Mashable	3
Mathway	20
MGM Resorts	44
Minted	17
MrExcel	1
NetProspex	4
OGUsers	1
OnlineSpambot	1
People Data Labs	1010
Petflow	11
Pluto TV	6
PoliceOne	1
Promo	1
Quidd	2
Reincubate	2
RiverCity Media	1
Scentbird	20
Slickwraps	2
Sonicbirds	1
Star Tribune	160
Straffic	130
StreetEasy	1
Ticketfly	1
TrikSpambotnet	4
TrueFire	3
VerificationsIO	22
Wattpad	22
Wishbone	8
YouveBeenScraped	7
Zoosk	21
Zynga	371

Appendix C: Management's Comments



UNITED STATES POSTAL SERVICE

May 5, 2021

Joseph Wolski
Director, Audit Operations

SUBJECT: Audit Report – *Integrity of the U.S. Postal Service's Social Media Presence* (Project Number 20-278-DRAFT)

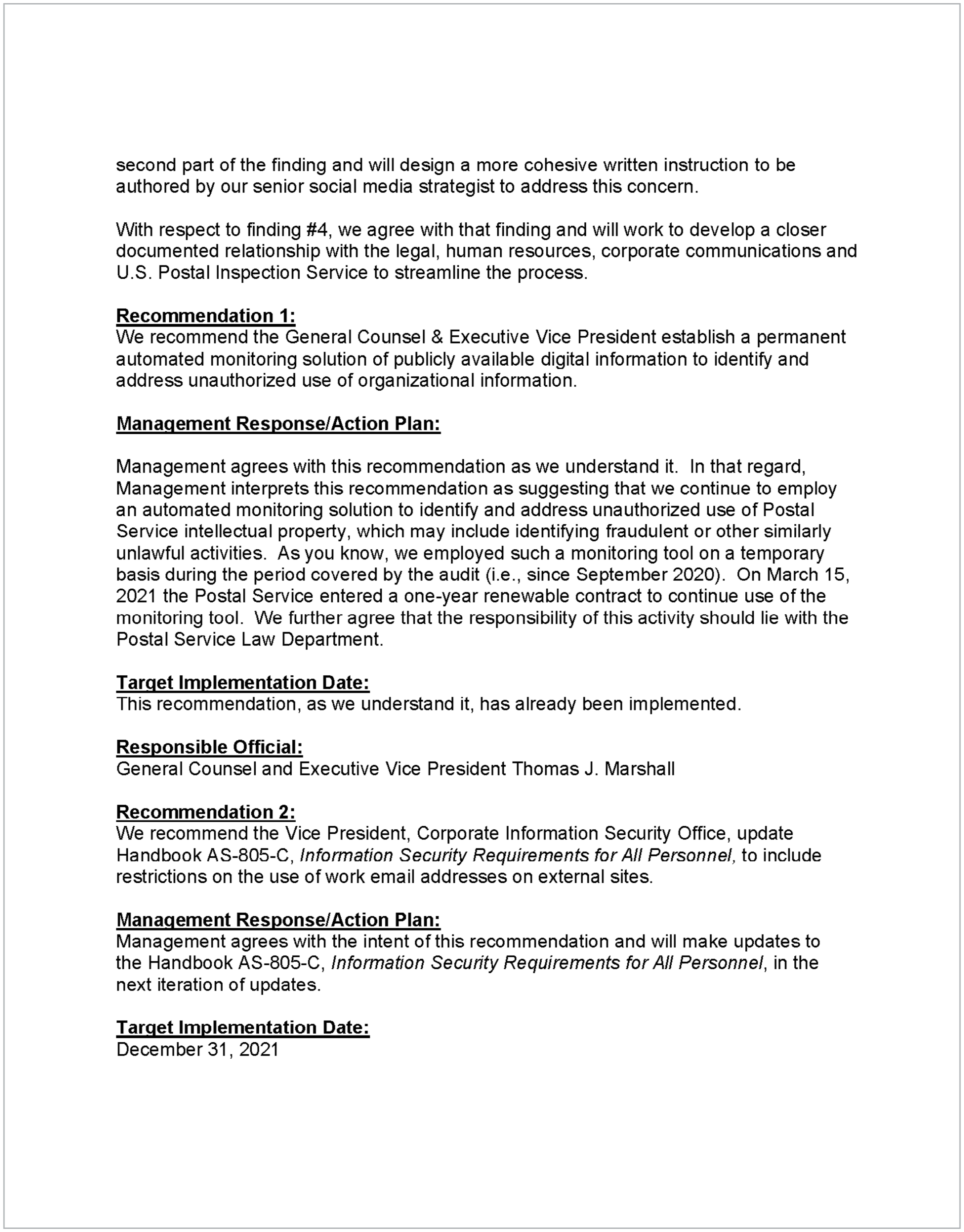
Introduction:
Thank you for the opportunity to work with your team as well as review and comment on the OIG Audit - *Integrity of the U.S. Postal Service's Social Media Presence.* (Project Number 20-278-DRAFT)

The Postal Service and its social and digital management teams are committed to providing safe and secure platforms for their customers and employees while navigating the social and digital space. We welcomed the valuable assessment the Office of the Inspector General provided with their audit teams.

With respect to finding #1, we do agree there is room to improve overall monitoring on social and other digital channels but it was not noted that the Postal Service, given limited resources and staffing, has indeed made inroads and worked with social platform providers to take down sites that were not deemed authentic. Since the commencement of the audit, the Postal Service Social and Digital Teams, along with our partners in the Law Department, have funded a tool that automates some aspects of social and digital traffic. The Law Department, along with the social and digital teams are being trained to effectively use this to further protect customers and employees. As we understand it, this target has now been met.

With respect to finding #2, the CISO team, responsible for this aspect of the audit, agrees with the finding.

With respect to finding #3, the Postal Service partially agrees because it is a two-part finding. Part one – the OIG audit indicated that Post Offices as well as USPS Sales teams set up unapproved sites, with the root cause being no automated monitoring of unapproved sites. However, the report does not point out that employees are required to follow ASM 363, the official USPS Social Media Policy document. The Postal Service has communicated over time through standup talks and electronic publications the importance of abiding by the approved and official social media policy. Given the fact that USPS employees over 644,000 employees and less than 30 unapproved sites were found, we believe the communication of our policy has indeed been effective. We will agree with the



second part of the finding and will design a more cohesive written instruction to be authored by our senior social media strategist to address this concern.

With respect to finding #4, we agree with that finding and will work to develop a closer documented relationship with the legal, human resources, corporate communications and U.S. Postal Inspection Service to streamline the process.

Recommendation 1:
We recommend the General Counsel & Executive Vice President establish a permanent automated monitoring solution of publicly available digital information to identify and address unauthorized use of organizational information.

Management Response/Action Plan:

Management agrees with this recommendation as we understand it. In that regard, Management interprets this recommendation as suggesting that we continue to employ an automated monitoring solution to identify and address unauthorized use of Postal Service intellectual property, which may include identifying fraudulent or other similarly unlawful activities. As you know, we employed such a monitoring tool on a temporary basis during the period covered by the audit (i.e., since September 2020). On March 15, 2021 the Postal Service entered a one-year renewable contract to continue use of the monitoring tool. We further agree that the responsibility of this activity should lie with the Postal Service Law Department.

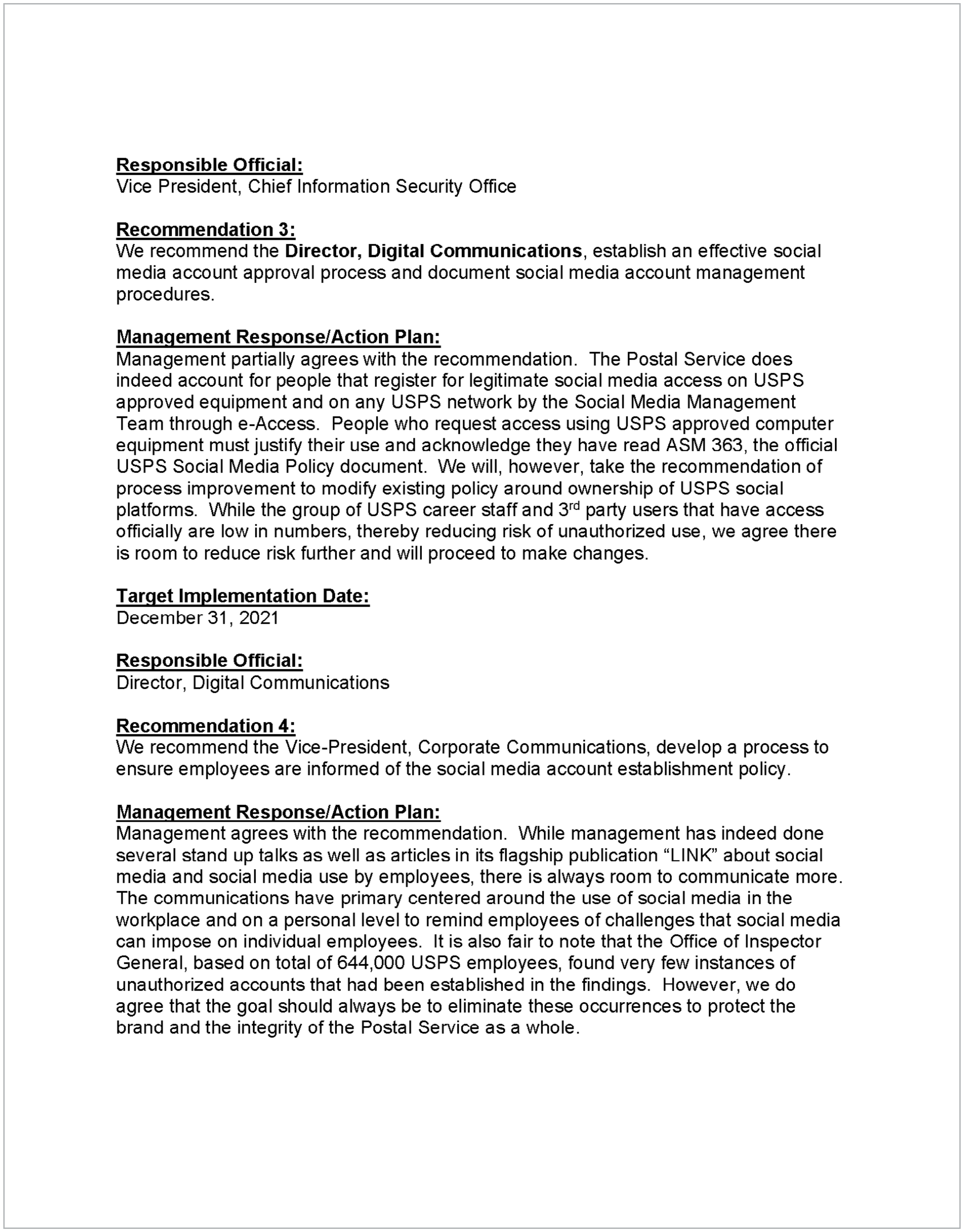
Target Implementation Date:
This recommendation, as we understand it, has already been implemented.

Responsible Official:
General Counsel and Executive Vice President Thomas J. Marshall

Recommendation 2:
We recommend the Vice President, Corporate Information Security Office, update Handbook AS-805-C, *Information Security Requirements for All Personnel*, to include restrictions on the use of work email addresses on external sites.

Management Response/Action Plan:
Management agrees with the intent of this recommendation and will make updates to the Handbook AS-805-C, *Information Security Requirements for All Personnel*, in the next iteration of updates.

Target Implementation Date:
December 31, 2021



Responsible Official:
Vice President, Chief Information Security Office

Recommendation 3:
We recommend the **Director, Digital Communications**, establish an effective social media account approval process and document social media account management procedures.

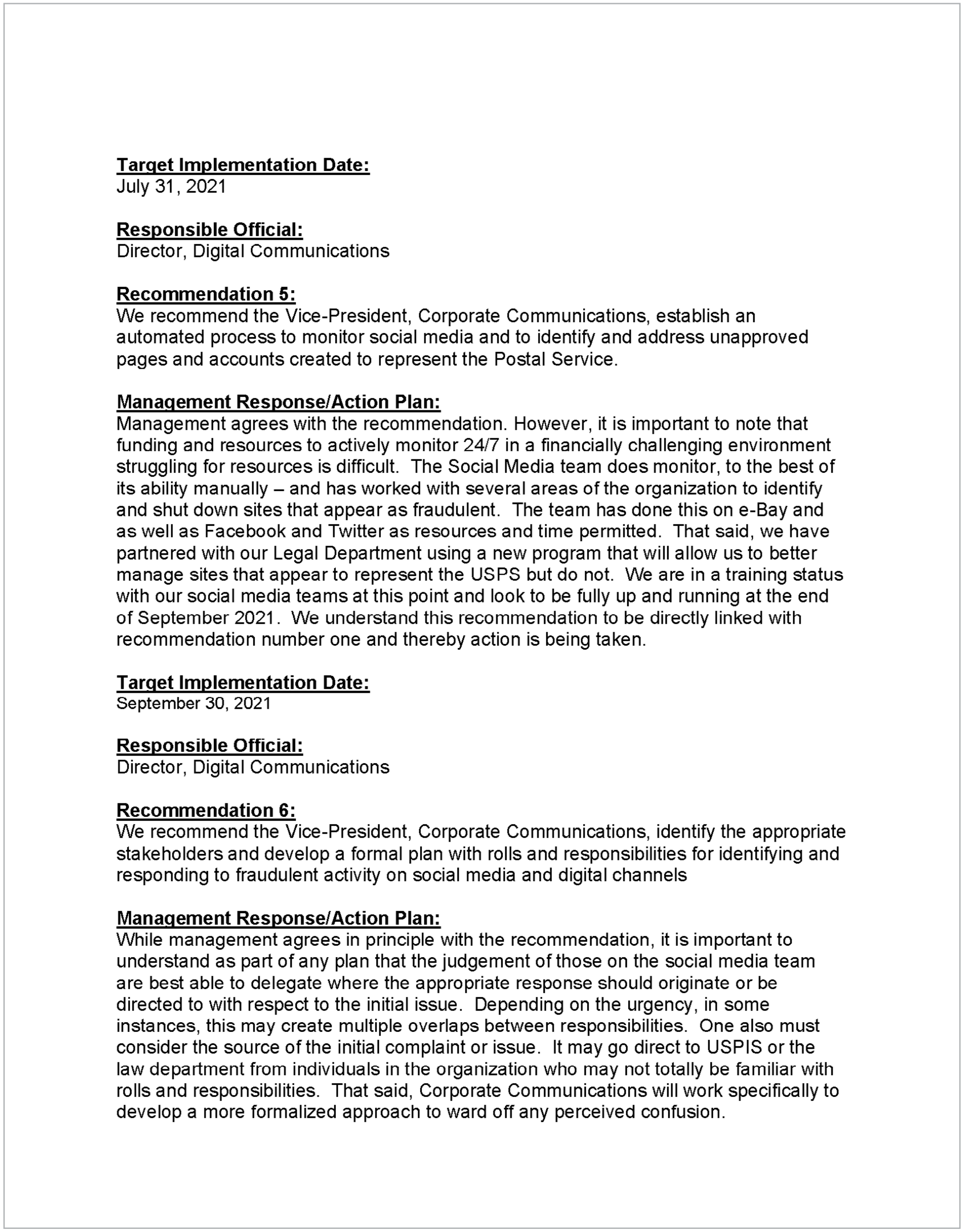
Management Response/Action Plan:
Management partially agrees with the recommendation. The Postal Service does indeed account for people that register for legitimate social media access on USPS approved equipment and on any USPS network by the Social Media Management Team through e-Access. People who request access using USPS approved computer equipment must justify their use and acknowledge they have read ASM 363, the official USPS Social Media Policy document. We will, however, take the recommendation of process improvement to modify existing policy around ownership of USPS social platforms. While the group of USPS career staff and 3rd party users that have access officially are low in numbers, thereby reducing risk of unauthorized use, we agree there is room to reduce risk further and will proceed to make changes.

Target Implementation Date:
December 31, 2021

Responsible Official:
Director, Digital Communications

Recommendation 4:
We recommend the Vice-President, Corporate Communications, develop a process to ensure employees are informed of the social media account establishment policy.

Management Response/Action Plan:
Management agrees with the recommendation. While management has indeed done several stand up talks as well as articles in its flagship publication “LINK” about social media and social media use by employees, there is always room to communicate more. The communications have primary centered around the use of social media in the workplace and on a personal level to remind employees of challenges that social media can impose on individual employees. It is also fair to note that the Office of Inspector General, based on total of 644,000 USPS employees, found very few instances of unauthorized accounts that had been established in the findings. However, we do agree that the goal should always be to eliminate these occurrences to protect the brand and the integrity of the Postal Service as a whole.



Target Implementation Date:
July 31, 2021

Responsible Official:
Director, Digital Communications

Recommendation 5:
We recommend the Vice-President, Corporate Communications, establish an automated process to monitor social media and to identify and address unapproved pages and accounts created to represent the Postal Service.

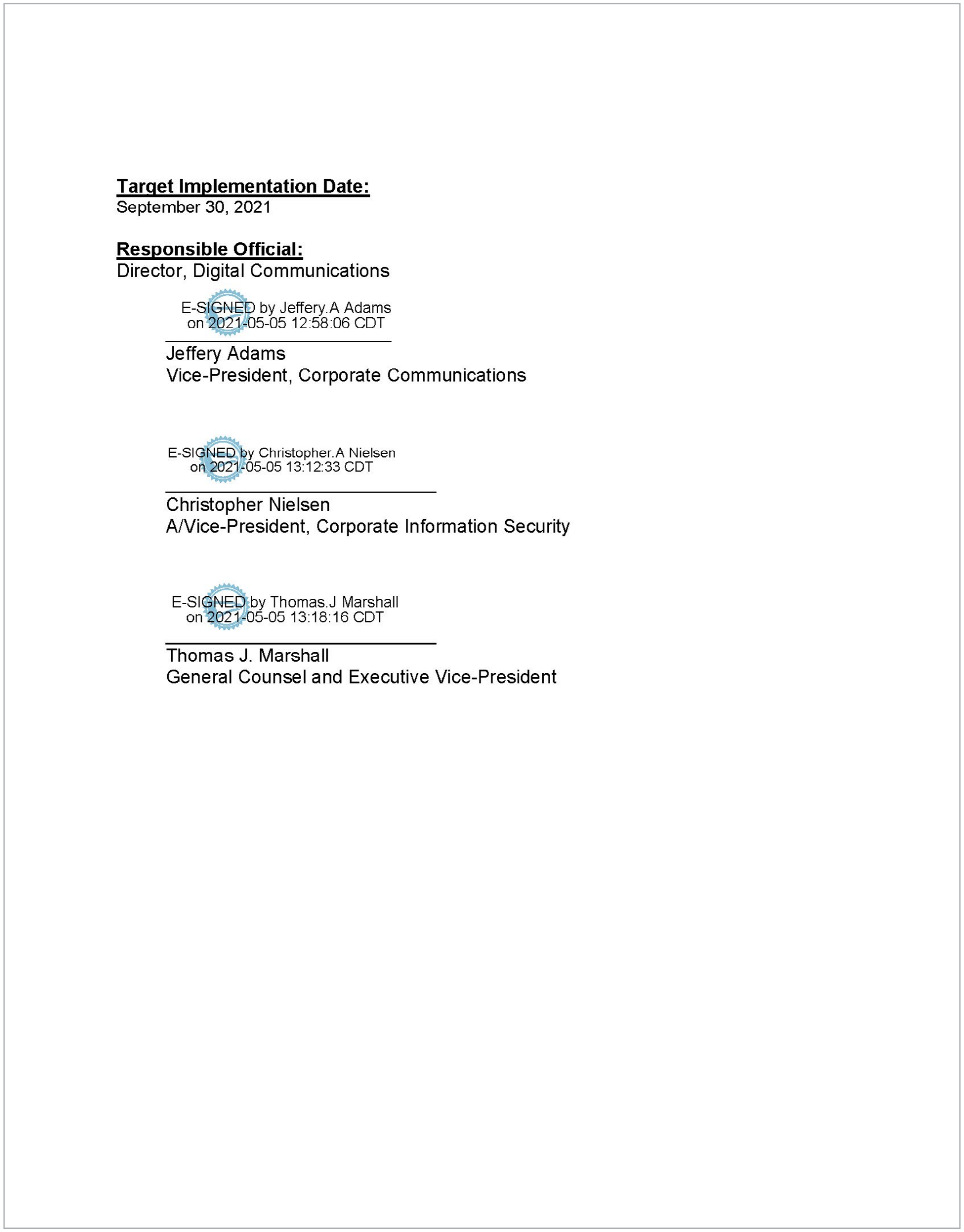
Management Response/Action Plan:
Management agrees with the recommendation. However, it is important to note that funding and resources to actively monitor 24/7 in a financially challenging environment struggling for resources is difficult. The Social Media team does monitor, to the best of its ability manually – and has worked with several areas of the organization to identify and shut down sites that appear as fraudulent. The team has done this on e-Bay and as well as Facebook and Twitter as resources and time permitted. That said, we have partnered with our Legal Department using a new program that will allow us to better manage sites that appear to represent the USPS but do not. We are in a training status with our social media teams at this point and look to be fully up and running at the end of September 2021. We understand this recommendation to be directly linked with recommendation number one and thereby action is being taken.

Target Implementation Date:
September 30, 2021

Responsible Official:
Director, Digital Communications

Recommendation 6:
We recommend the Vice-President, Corporate Communications, identify the appropriate stakeholders and develop a formal plan with rolls and responsibilities for identifying and responding to fraudulent activity on social media and digital channels

Management Response/Action Plan:
While management agrees in principle with the recommendation, it is important to understand as part of any plan that the judgement of those on the social media team are best able to delegate where the appropriate response should originate or be directed to with respect to the initial issue. Depending on the urgency, in some instances, this may create multiple overlaps between responsibilities. One also must consider the source of the initial complaint or issue. It may go direct to USPIS or the law department from individuals in the organization who may not totally be familiar with rolls and responsibilities. That said, Corporate Communications will work specifically to develop a more formalized approach to ward off any perceived confusion.



Target Implementation Date:
September 30, 2021

Responsible Official:
Director, Digital Communications

E-SIGNED by Jeffery.A Adams
on 2021-05-05 12:58:06 CDT

Jeffery Adams
Vice-President, Corporate Communications

E-SIGNED by Christopher.A Nielsen
on 2021-05-05 13:12:33 CDT

Christopher Nielsen
A/Vice-President, Corporate Information Security

E-SIGNED by Thomas.J Marshall
on 2021-05-05 13:18:16 CDT

Thomas J. Marshall
General Counsel and Executive Vice-President

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 inquires please email
press@uspsoig.gov or call 703-248-2100.