Office of Inspector General | United States Postal Service

Management Advisory

Virtual Private Network Access

Report Number IT-MA-19-001 | August 19, 2019

Table of Contents

Highlights

Objective

Our objective was to evaluate whether virtual private network (VPN) access to the U.S. Postal Service's Information Technology (IT) network was granted only to those individuals who require access. eAccess is used for requesting and approving access for applications and other IT infrastructure. We reviewed eAccess data that showed authorizations for Postal Service contractors and employees who have been granted VPN access.

VPN provides users with a means to securely access information on a corporate network infrastructure or an untrusted public network (e.g., the Internet). On [redacted]. The Postal Service now uses VPN to provide users with a means to securely access information on its IT network from a remote location.

"It is important to provide VPN access in a manner that reduces the risk of security complexities associated with remote access."

One of the primary IT security challenges with VPN is limiting unnecessary access to critical business applications and network resources. It is important to establish justifiable business rules and monitor VPN permissions to reduce the risk of IT security complexities associated with remote access to networks. As of March 15, 2019, [redacted] contractors and [redacted] Postal Service employees had authorized VPN access.

What the OIG Found

We identified contractors and bargaining employees with VPN access to the Postal network that had access higher than permitted by Postal Service policy. We identified [redacted] of the [redacted] (about 28 percent) contractor personnel had a higher level of VPN access than what Postal Service policy permits. Postal Service policy states that contractors should not have a higher level of VPN access unless they had been issued a Postal Service device. In addition, there were [redacted] bargaining employees with authorized VPN access to the Postal Service IT network. While this does not represent a significant number of employees, [redacted]

VPN access approvals are controlled by a user's eAccess approving manager, who determines the level of access based on the business need. There are no controls within eAccess to identify for the approving manager those instances where VPN access may not be appropriate for the user. It is important to provide VPN access in a manner that reduces the risk of security complexities associated with remote access. However, Postal Service plans to invest [redacted] million into an eAccess Technology Refresh and Privileged Access Management program. This investment into a modern access management system will address concerns related to managing authorizations to the IT network.

What the OIG Recommended

We recommended the Postal Service analyze its contractors and bargaining employees with VPN access and make appropriate changes.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

August 19, 2019

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

PRITHA N. MEHRA
VICE PRESIDENT, INFORMATION TECHNOLOGY

FROM: Jason M. Yovich
Acting Deputy Assistant Inspector General
for Technology

SUBJECT: Management Advisory Report – Virtual Private Network Access (Report Number IT-MA-19-001)

This report presents the results of our review regarding potential Virtual Private Network (VPN) Access vulnerabilities to the U.S. Postal Service Information Technology network (Project Number 19TG008IT000). Specifically, we reviewed Postal Service employee and contractor VPN access.

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

Attachment

cc: Postmaster General
Corporate Audit Response Management

Results

Introduction/Objective

This management advisory report presents the results of our self-initiated review of virtual private network (VPN) access. Our objective was to evaluate whether VPN access to the U.S. Postal Service's Information Technology (IT) network was granted only to those individuals who require access. eAccess is used for requesting and approving access for applications and other IT infrastructure. We reviewed eAccess data that shows authorizations for those Postal Service contractors and employees who have been granted VPN access.

Background

As part of the Postal Service's mission to strengthen the security of its network, management took measures to limit external access from unauthorized and/or malicious actors. On [redacted] The Postal Service now uses VPN to provide users with a means to securely access information on its IT network from a remote location. An important concept in computer security is the principle of least privilege, which is the practice of limiting access rights for users to the bare minimum permissions they need to perform their work. Access level determines the specific network resources that users can access. The Postal Service restricts remote access privileges to authorized personnel and appropriate management must approve these privileges through eAccess before they are granted.[1]

While VPN is a secure connection capability, it comes with inherent issues and management challenges regarding application of the concept of least privilege. One of the primary IT security challenges with VPN is limiting unnecessary access to critical business applications and network resources. It is important to establish justifiable business rules and monitor VPN permissions to reduce the risk of IT security complexities associated with remote access to networks. This is especially true when organizations allow remote access privileges to business partners (i.e., contractors). As of March 15, 2019, [redacted] contractors and [redacted] Postal Service employees had authorized VPN access.

Finding #1: Contractors With Virtual Private Network Access

The *VPN Access BP - 2FA* is the request contractors use to gain VPN Access to the Postal Service network in eAccess. This is different from the *VPN Access to USPS - 2FA* request contractors submit, which allows full access to the network.[2] Contractors authorized with *VPN Access to USPS - 2FA* must use a Postal Service issued device to connect remotely, otherwise, the contractor must use *VPN Access BP - 2FA.*

We identified [redacted] contractors who did not have a Postal Service laptop/mobile media record within eAccess but had *VPN Access to USPS - 2FA* access. Figure 1 shows a breakdown of the [redacted] contractors that do not have an authorized Postal Service computing device.

> *"One of the primary IT security challenges with VPN is limiting unnecessary access to critical business applications and network resources."*

1 Handbook AS-805, *Information Security,* Section 11-9, Remote Access Requirements, December 2018.

2 The *VPN Access BP - 2FA* resource in eAccess records all Business Partners who are approved for a specialized version of remote VPN access to the Postal Service network. The *VPN Access to USPS - 2FA* is for employees of any company to receive full access to the Postal Service Network. Source: USPS Knowledge Base Article 43978, VPN Access BP - Instructions for the version of VPN used by Business Partners, dated May 2, 2016.

Figure 1. Top Vendors with Contractors Having VPN Access to USPS - 2FA Access

Sou

Postal Service policy states that contractors (also referred to as Business Partners) must have limited access to the information resources stated in their Network Connectivity Review Board request.[3] Additionally, Postal Service policy states that if a contractor has a non-Postal Service device they must use *VPN Access BP - 2FA* to connect to the network.[4] Postal Service guidance also states that contractor access is restricted because management wants to guard the network from possibly compromised devices that the Postal Service has no control over.

This occurred because a contractor's access level is approved by their eAccess approving manager and there is no control within eAccess to flag that only *VPN Access to USPS - 2FA* should be given to contractors who also have a Postal Service issued device. The appropriate level of access is important to ensure administrative procedures and controls protect Postal Service information resources. Restricting access from users who do not have a Postal Service device is important to guard the network from possibly compromised devices that the Postal Service has no control over.

We are not making a recommendation to change eAccess to flag contractors requesting VPN access because the Postal Service plans to invest [redacted] million into an eAccess Technology Refresh and Privileged Access Management program. This investment into a modern access management system will address concerns related to managing authorizations to the IT network.

> *"Restricting access from users who do not have a Postal Service device is important to guard the network from possibly compromised devices that the Postal Service has no control over."*

Recommendation #1:

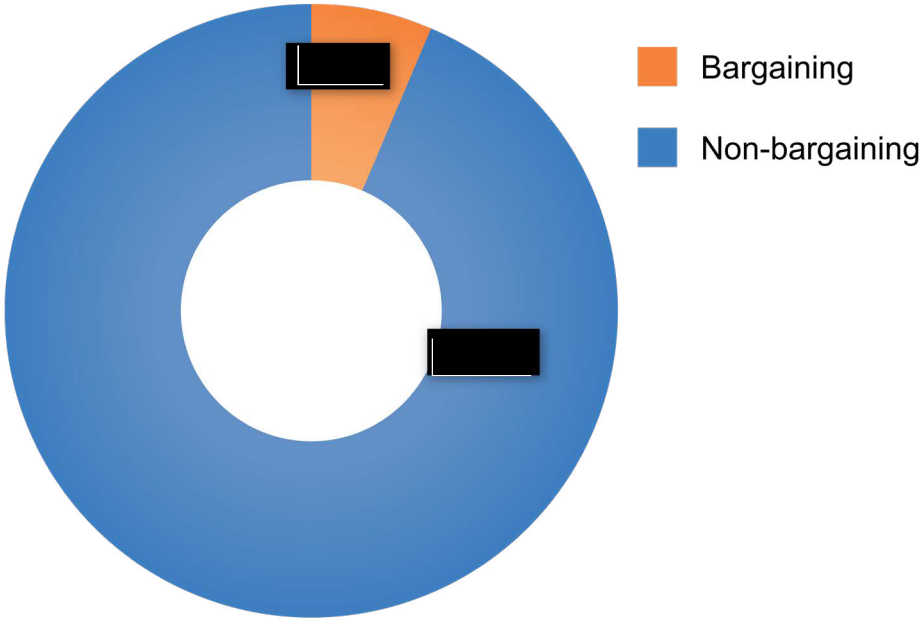
We recommend the **Vice President, Information Technology, in coordination with the Vice President, Chief Information Security Officer,** periodically analyze Postal Service contractors with authorized VPN Access to USPS - 2FA access to ensure that they are issued a Postal Service device and make changes as appropriate.

3 Handbook AS-805, Section 11-7, Business Partner Connectivity Requirements, December 2018.
4 Knowledge Base Article 43978, *VPN ACCESS BP – Instructions for the Version of VPN Used by Business Partners,* May 2, 2016.

Finding #2: Bargaining Employees with Virtual Private Network Access

As of March 15, 2019, we identified [redacted] Postal Service employees with authorized VPN access in eAccess. Figure 2 shows [redacted] bargaining and [redacted] non-bargaining employees with authorized VPN access.[5]

Figure 2. Bargaining vs. Non-Bargaining



Source: eAccess and job descriptions online.

We identified [redacted] bargaining employees with authorized VPN access to the Postal Service IT network. While this does not represent a significant number of employees, due to the nature of their work, [redacted] We identified carriers, tractor trailer operators, and maintenance mechanics who had VPN access.[6] According to Postal Service policy, VPN access must be governed by the principle of least privilege and limited to those services and devices needed to perform the business function requested.[7]

[redacted]

This most likely occurred because bargaining employees' eAccess managers were approving VPN access without considering whether or not it was appropriate for their position. Limiting VPN access to only those employees who need it to perform their business function is an important control to reduce the risk of potential security issues associated with remote access.

> *"Limiting VPN access to only those employees who need it to perform their business function is an important control to reduce the risk of potential security issues associated with remote access."*

Recommendation #2:

We recommend the **Vice President, Information Technology, in coordination with the Vice President, Chief Information Security Officer,** analyze Postal Service bargaining employees with authorized Virtual Private Network access and coordinate with their supervisors to make appropriate changes.

5 Bargaining employees are represented by labor unions or other labor organizations that negotiate with the government to ensure favorable employment conditions and fair wages.
6 All postal employees have access to certain applications such as their career development, payroll, and service performance using https://liteblue.usps.gov, which does not require VPN access.
7 Handbook AS-805, Section 11-8, Limiting Third-Party Network Services, dated December 2018.
8 Handbook EL-903, *Agreement Between the United States Postal Service and the National Mail Handlers A Division of Laborers'International Union of North America, AFL-CIO,* Section 8.5, Overtime Assignments, dated 2016-2019 & Handbook EL-908, *Agreement Between the United States Postal Service and the American Postal Workers Union, AFL-CIO Covering Information Technology/Accounting Services,* Section 8.05, Overtime Assignments, dated 2017-2019.

Management's Comments

Management agreed with all of the findings in the report.

Regarding recommendation 1, management stated they will review and update references to the information security policy that apply to VPN access to reinforce language that specifies that use of a postal device to access the network is a requirement. Management plans to complete these actions by January 2020.

Regarding recommendation 2, management stated they will add a requirement to review VPN access for Postal Service employees to the eAccess Manager Periodic Review process. Management plans to complete this by October 2019.

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

Evaluation of Management's Comments

The OIG considers management's comments responsive to recommendation 2 and the corrective actions should resolve the issue identified in the advisory. The OIG considers management's comments to recommendation 1 to be non responsive and will not resolve the issue identified in the advisory.

Regarding recommendation 1, management stated they will review and update references to the information security policy that apply to VPN access. In lieu of analyzing the [redacted] contractors, management stated they would rely on their mitigating control, which is designed to prevent non-Postal Service devices from connecting to the network. We believe management should periodically analyze Postal Service contractor VPN access, including the contractors we identified, rather than relying solely on their mitigating control to guard the network from possibly compromised devices.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. Recommendations should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

Appendices

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

Appendix A: Additional Information

Scope and Methodology

The scope of this management advisory was Postal Service employees and contractors who were granted VPN access as of March 2019.

To accomplish our objective, we:

- Obtained and analyzed data generated from eAccess to determine what level of VPN access was granted to Postal Service employees and contractors and whether Postal Service laptop/mobile media devices were issued to contractors.
- Reviewed VPN security policies, processes, and procedures.
- Met with Postal Service management and representatives that manage VPN access.

We conducted this review from March through August 2019, 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 work to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our 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 conclusion with management on July 22, 2019, and included their comments where appropriate.

We assessed the reliability of data from the eAccess system by comparing its data for names and occupation titles to the global address list in Outlook and the employee master file. We determined that the data were sufficiently reliable for the purposes of this advisory.

Prior Audit Coverage

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

Appendix B: Management's Comments

UNITED STATES POSTAL SERVICE

August 8, 2019

Lazerick Poland
Director, Audit Operations

SUBJECT: Management Advisory – Virtual Private Network Access
(Report Number IT-MA-19-DRAFT)

US Postal management agrees with both findings as noted below. Security is very important and controls are in place whereby an ACE computer is required for VPN 2FA access to connect to our USPS systems. There are instances where Bargaining Unit employees have positions that require VPN 2FA access and this access is approved by their supervisors in eAccess. Based on this information, our responses, activities and target dates are listed below.

Recommendation #1:
We recommend the **Vice President, Information Technology, in coordination with the Vice President, Chief Information Security Officer**, periodically analyze Postal Service contractors with authorized *VPN Access to USPS - 2FA* access to ensure that they are issued a Postal Service device and make changes as appropriate.

Management Response/Action Plan:
Management agrees with the OIG that contractors using VPN Access to USPS - 2FA must use USPS provided devices to connect to the network. The system is designed to not allow a non-USPS device to connect. In light of this, CISO and IT will review and update references to the Information Security policy that apply to VPN access to reinforce language that specifies that use of a postal device to access the network is a requirement.

Target Implementation Date:
January 31, 2020

Responsible Official:
Manager, Enterprise Access Infrastructure and Manager, Deputy Chief Information Security Office

Recommendation #2:
We recommend the **Vice President, Information Technology, in coordination with Vice President, Chief Information Security Officer,** analyze Postal Service bargaining

employees with authorized Virtual Private Network access and coordinate with their supervisors to make appropriate changes.

Management Response/Action Plan:
Management agrees with the OIG that users having *VPN Access to USPS - 2FA* should periodically be reviewed. CISO and IT will add a requirement for the review of VPN 2 FA access for Postal employees to the eAccess Manager Periodic Review process.

Target Implementation Date:
October 31, 2019

Responsible Official:
Manager, Enterprise Access Infrastructure and Manager, Digital Integration

Gregory S. Crabb
Vice President, Chief Information Security Officer

Pritha N. Mehra
Vice President, Information Technology

cc: *copy those that were copied on the OIG draft audit report, plus*
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, contact Agapi Doulaveris
Telephone: 703-248-2286
adoulaveris@uspsoig.gov