Security of Electric Vehicle Charging Stations

AUDIT REPORT

Report Number 24-020-R25 | June 5, 2025

Table of Contents

Highlights

Background

The U.S. Postal Service operates one of the largest civilian delivery fleets in the world, with more than 232,000 vehicles delivering to nearly 169 million addresses across the country. As part of its 10-year strategic plan, it is modernizing its 30-year-old fleet to a mix of internal combustion engine (gas) and electric vehicles (EV). To support this effort, the Postal Service contracted with three vendors in February 2023 to purchase 14,050 EV charging stations and commissioned 3,925 charging stations as of March 2025. The overall security and functionality of EV charging stations is critical to ensure the Postal Service's EVs are available to deliver mail.

What We Did

Our objective was to assess the security of the Postal Service's EV charging stations. We contracted with a provider to evaluate the technical, communication, and data security controls of one charging station from each of the three vendors. We also conducted site visits to Sorting and Delivery Centers at [redacted] to review physical security for safeguarding EV charging stations and evaluated policies and best practices for contingency planning.

What We Found

The charging stations had security risks that could disrupt EV charging or allow unauthorized charging sessions. In addition, security cameras at the selected sites we visited were either not 1) installed; 2) accessible to management; or 3) monitoring the charging stations. Finally, there were inadequate contingency plans for charging stations to charge EVs during prolonged power outages or charging station functionality issues.

Recommendations and Management's Comments

We made seven recommendations to address the issues related to charging station vulnerabilities, physical security, and contingency planning identified in the report. Postal Service management agreed with four recommendations and disagreed with three. Management's comments and our evaluation are at the end of each finding and recommendation. The U.S. Postal Service Office of Inspector General (OIG) considers management's comments nonresponsive to recommendations 1, 2, and 3 and will work with management through the formal audit resolution process. The OIG considers management's comments responsive to recommendations 4, 5, 6, and 7, as corrective actions should resolve the issues identified in the report. See Appendix B for management's comments in their entirety.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

June 5, 2025

MEMORANDUM FOR:

RONNIE J. JARRIEL
CHIEF LOGISTICS AND INFRASTRUCTURE OFFICER AND
EXECUTIVE VICE PRESIDENT

GARY BARKSDALE
CHIEF POSTAL INSPECTOR

BENJAMIN P. KUO
VICE PRESIDENT FACILITIES

VICTORIA K. STEPHEN
EXECUTIVE DIRECTOR OF THE NEXT GENERATION DELIVERY
VEHICLE PROGRAM

RAE ANN HAIGHT
DIRECTOR OF OFFICE OF NATIONAL PREPAREDNESS

JOHN S. MORGAN
VICE PRESIDENT DELIVERY OPERATIONS

Mary K. Lloyd

FROM: Mary Lloyd
Deputy Assistant Inspector General
for Inspection Service and Cybersecurity & Technology

SUBJECT: Audit Report - Security of Electric Vehicle Charging Stations
(Report Number 24-020-R25)

This report presents the results of our audit of the Security of Electric Vehicle Charging Stations.

All recommendations require U.S. Postal Service Office of Inspector General's (OIG) concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. Recommendations 1, 2, 3, 4, 6, and 7 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 5 closed with issuance of this report.

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

Attachment

cc: Postmaster General
Corporate Audit Response Management

Results

Introduction/Objective

This report presents the results of our self-initiated audit of the Security of Electric Vehicle Charging Stations (Project Number 24-020). Our objective was to assess the technical and physical security of the U.S. Postal Service electric vehicle (EV) charging stations. See Appendix A for additional information about this audit.

Background

The Postal Service operates one of the largest civilian delivery fleets in the world, with more than 232,000 vehicles delivering to nearly 169 million addresses across the country. As part of its 10-year strategic plan, Delivering For America: Our Vision and Ten-Year Plan to Achieve Financial Sustainability and Service Excellence, the Postal Service is modernizing its 30-year-old fleet to a mix of internal combustion engine (gas) vehicles and EVs. In August 2022, the Postal Service received funding as part of the Inflation Reduction Act[1] to purchase zero-emission delivery vehicles and to install related infrastructure. The Postal Service announced that it expects to acquire 66,000 EVs, with at least 45,000 being Next Generation Delivery Vehicles[2] (NGDV), by 2028. The remaining 21,000 vehicles will be purchased as commercial-off-the-shelf EVs to meet immediate delivery needs and requirements. As of March 2025, there were 36 electric NGDVs and 823 commercial-off-the-shelf EVs commissioned on routes, for a total of 859 EVs in use. The overall security and functionality of EV charging stations is critical to ensure the Postal Service's EVs are available to deliver mail.

In February 2023, to support modernizing its fleet to EVs, the Postal Service awarded $74 million in contracts to three vendors to purchase 14,050 EV charging stations. As of March 2025, the Postal Service had over 3,900 charging stations to support its electric fleet deployed at new Sorting and Delivery Centers (S&DC)[3] to complement its network modernization plans. S&DCs are operational in several areas across the country and are, as new facilities, more likely to support power and infrastructure needs than older facilities, thus requiring less infrastructure upgrades as they prepare for EV deployment.

According to the NGDV Program Management Office, they are tasked with the planning, development, and implementation of EV charging infrastructure, including the procurement of charging stations. Additionally, they frequently meet with all three vendors to discuss issues, updates, and deployment progress.

The Postal Service's Facilities team works with the Postal Inspection Service to craft building and site security requirements. The Inspection Service is tasked with evaluating and approving security-related equipment such as closed-circuit television security cameras (CCTV) at facilities. Also, they develop a site risk profile and security-risk analysis that determines the need for certain security products and services. Physical access to EV charging stations is required to exploit most vulnerabilities that would disrupt charging services, making physical security imperative.

Because EVs and charging stations are critical assets to the Postal Service's operations and represent large investments in network and fleet modernization, contingency planning is imperative to prevent service interruptions and to support emergency and disaster response, such as establishing alternative power sources. To assist Postal Service operations, the National Preparedness office has tools and resources to assist local management during emergency situations. Contingency planning, alongside physical security of charging stations, can serve as part of a wider strategic plan that supports the Postal Service's mission to deliver the mail.

1 A recent Executive Order titled Unleashing American Energy (issued on January 20, 2025) described, among other things, the new administration's policies related to government funding for EVs. Federal Register: Unleashing American Energy Our audit work was substantially completed prior to the issuance of the order.
2 A combination of battery EVs and internal combustion, low emission vehicles that are custom built for Postal Service needs and specifications
3 Units that combine several delivery facilities into a single larger facility that services multiple ZIP codes in a geographic area. These facilities are part of the broader Delivering for America plan.

To test technical and physical security of the Postal Service's charging stations, we engaged a contractor with subject matter expertise to assess technical controls, communication protocols, data security, and vulnerabilities on one charging station from each of the three vendors. The contractor performed 24 security tests, as follows:

- Ten tests for physical security of technical controls.
- Seven tests for communication protocols and data security.
- Seven tests for vulnerabilities of charging station firmware.

Although an ongoing audit[4] identified ongoing operability issues with Vendor One's charging stations, we opted to conduct security testing of their charging station. According to Vendor One, the firmware code and core components of the model tested are identical to the Postal Service's model. We did not verify that the configuration settings on the model tested mirrored the Postal Service's; however, Vendor One confirmed that the configuration settings would not negate the vulnerabilities identified during testing. For Vendors Two and Three, the vendors confirmed that the models, firmware, and configuration settings on the models tested were identical to those in use by the Postal Service.

Currently, two of three vendors are Federal Risk and Authorization Management Program certified, which is a program that promotes secure cloud services across the Federal government by standardizing the approach to security and risk assessment for cloud technologies. However, the focus of this effort was on the EV charging stations, and as such we did not assess the vendors' cloud systems.

Findings Summary

While the Postal Service made efforts to reduce potential security risks to its EV charging stations, we identified opportunities for improvement regarding technical and physical security of the charging stations and contingency operations. Specifically, we identified charging station vulnerabilities that require physical access to exploit. Additionally, we observed that the S&DC in [redacted] did not have security cameras installed, and the S&DCs in [redacted] and [redacted] did not have cameras properly installed. Finally, there were inadequate contingency plans in place if charging stations become nonfunctioning due to extended periods of power outages.

4 Fleet Modernization: Facility Preparedness for Electric Vehicles at the [redacted]

Finding #1: EV Charging Station Vulnerabilities

We identified charging station vulnerabilities from all three vendors tested that can impact their operation, allow for misuse of Postal Service property, and could impede the Postal Service's ability to deliver the mail. However, the identified weaknesses require physical access to the charging stations to exploit these risks.

Vendor One

Vendor One's charging stations had the highest risk of disruption of service. Specifically, during our testing, we:

- Extracted and altered the firmware,[5] which allowed reprogramming of the charging station. Specifically, the [redacted] that handles charging [redacted] and can be exploited to render a charging station unusable.
- Accessed the [redacted] data, which allowed [redacted] of the [redacted]. Vendor One confirmed that the [redacted] tested was identical to the [redacted] the Postal Service uses.

According to Postal Service policy.[6] information resources must be protected against damage, unauthorized access, and theft in the Postal Service environment and when removed from this secure environment. Additionally, policy[7] states that [redacted] must be protected from unauthorized use.

We were able to reprogram the charging station because it [redacted] methods to verify firmware updates. Also, we were able to [redacted] the [redacted] because Vendor One used [redacted] to protect the [redacted] data; however, that put the [redacted] at risk of easily being [redacted] because the [redacted] is well known to bad actors.

As a result of the contractor's work, Vendor One will be reporting the [redacted] vulnerability (and one other vulnerability identified, but not applicable to the Postal Service) to the [redacted] database.[8]

Vendor Two

During testing of Vendor Two's charging station, we were able to disrupt charging, access the service menu, and gain unauthorized access via [redacted] loopholes. Also, the [redacted] in the [redacted] could be [redacted] using other devices and [redacted].

We were able to disrupt charging by accessing the charging station's service menu through a [redacted] with customizable hardware via the [redacted] which is a publicly available [redacted]. This menu provides the ability to initiate a free charging session, reboot the system, or restore the charging station to factory defaults.

Additionally, we were able to break into the [redacted] and gain unauthorized access to charging, essentially allowing any user to charge an EV. Finally, we [redacted] the [redacted] of the authorized [redacted], which provided us access to the charging station.

According to Postal Service policy,[11] facilities, equipment, services, protocols, and applications used to transmit, store, and process information

> "As a result of the contractor's work, Vendor One will be reporting the [redacted] vulnerability to the [redacted] database.

5 Computer programs and data stored in hardware that can be dynamically modified during execution.
6 AS 805 Information Security 7-4 Physical Protection of Information Resources.
7 AS 805 Information Security [redacted]
8 [redacted]
9 [redacted]
10 [redacted]
11 AS 805 Information Security 11-1.2 Network Infrastructure.

must be protected through specific requirements, including physical security, identification and authentication, and authorization. Policy[12] also states that [redacted] must be protected from unauthorized use. Finally, best practices[13] recommend that data on [redacted] be encrypted to protect against unauthorized use.

These issues existed because the [redacted] did not have a [redacted] in place after a certain amount of failed login attempts to reduce the likelihood of a successful [redacted]. In addition, issues with unauthorized access occurred due to a setting that allows any [redacted] to initiate charging sessions when the charging station does not have network connectivity. Finally, although the Postal Service has taken steps to protect sensitive information by using a [redacted] instead of employee information for the [redacted] the [redacted] was not adequately protected with [redacted] using unauthorized devices and [redacted].

These vulnerabilities can allow any user to gain unauthorized access to charging sessions, access internal menus, and disrupt charging sessions for EVs, which can ultimately impact or even delay mail delivery.

Vendor Three

As with Vendor Two's vulnerability, we obtained the [redacted] from the [redacted] of the [redacted] using other devices and [redacted].

Policy[14] states that [redacted] must be protected from unauthorized use. Additionally, best practices[15] recommend that data on [redacted] be encrypted to protect against unauthorized use.

This occurred because the [redacted] was not protected adequately to prevent reuse on unauthorized devices and [redacted], which could allow any user to gain access to charging stations for unauthorized use, leading to further misuse of Postal Service property.

Without proper technical controls in place to safeguard charging stations, EVs may not be able to properly charge, which can lead to significant disruptions and delays to Postal Service's operations. However, because bad actors need physical access to the charging stations to exploit these vulnerabilities, the threat can be reduced by using physical security controls, such as fencing, gates, and security cameras.

Recommendation #1

We recommend that the **Chief Logistics and Infrastructure Officer and Executive Vice President**, work with Vendor One to remediate (or accept the risks associated with) the vulnerabilities identified with its charging stations.

Recommendation #2

We recommend that the **Chief Logistics and Infrastructure Officer and Executive Vice President**, work with Vendor Two to remediate (or accept the risks associated with) the vulnerabilities identified with its charging stations.

Recommendation #3

We recommend that the **Chief Logistics and Infrastructure Officer and Executive Vice President**, work with Vendor Three to remediate (or accept the risks associated with) the vulnerability identified with its charging stations.

Postal Service Response

The Postal Service disagreed with this finding and recommendations 1, 2, and 3.

Regarding the finding for Vendor One, management stated the level of risk and impact of the known vulnerability is minor, would be challenging to replicate in a secure, lighted,

12 AS 805 Information Security [redacted]
13 NIST Special Publication [redacted]
14 AS 805 Information Security [redacted]
15 NIST Special Publication [redacted]

fenced, operational postal facility, and the impact would be limited to a single charging station. Further, management stated that the fact that we were able to reprogram the charging station because it [redacted] methods to verify firmware updates is not accurate. The [redacted] that was attacked does not have [redacted]; those features reside on a [redacted], which constrains the impact to a single charging station. Vendor One acknowledged the vulnerability by stating: "the issue exists. It's low probability, minor impact, and easy to address."

For Vendor Two, management stated the audit report describes a [redacted] vulnerability, which would require the attacker to use a specific [redacted] and a [redacted] to apply the attack through a service menu. Vendor Two has acknowledged the issue and will be addressing it; however, the attack requires physical access, and its impact is limited to a single charging station. For this vendor, although management stated they disagree with this portion of the finding, their comments are in agreement with what we documented in the report.

For Vendor Three, management stated that the only issue identified was related to being able to [redacted] its [redacted] (which also applies to Vendors One and Two) to initiate charging sessions. Also, management stated that to [redacted] the [redacted] a bad actor would need access to one of the [redacted] which would be difficult because the [redacted] are assigned by vehicle and retained as an accountable item with the vehicle keys, which must be checked in and out by each carrier/driver every day, with every usage.

For recommendations 1, 2, and 3, management stated it disagrees and accepts the nominal risk of these low-probability, low impact, easy-to-address issues.

OIG Evaluation

Regarding the finding for Vendor One, the audit team and contractors provided technical support demonstrating that we did reprogram the the charging station because it [redacted] methods to verify firmware updates. Further, Vendor One confirmed this vulnerability exists and is exploitable, as cited in management's response to this finding, and issued a "[redacted]" release to address the identified vulnerability.

Regarding the finding for Vendor Three, a bad actor or insider threat could [redacted] the [redacted] from one of Postal's [redacted] to a [redacted] to establish an unauthorized charging session. In addition, accountable items — such as arrow keys, which are used to open blue mailboxes and cluster boxes — are lost or stolen all the time. So, [redacted] could also be lost or stolen, adding to the risk. The vendor is aware of this vulnerability and is working on a solution to improve the security of the [redacted]

The Postal Service disagreed with recommendations 1, 2, and 3 because it says it will accept the risk of the vulnerabilities identified with its charging stations. Although management stated they accept the risk associated with the vulnerabilities, they did not provide documentation or a target implementation date for the formal acceptance of the identified risks. We view management's disagreement with the recommendation as unresolved and will work with management though the formal audit resolution process.

Finding #2: Inadequate Physical Security of Charging Stations

We found that the [redacted] S&DCs had several physical security measures in place to protect and safeguard charging stations, such as fencing and gates. However, they did not have sufficient physical security controls, such as CCTVs in parking lot areas where EV charging stations were installed, to detect unauthorized access or use of charging stations.

Specifically, the [redacted] S&DC did not have any CCTVs installed. In [redacted] employees did not have the ability to monitor the video feed of the CCTVs. Although cameras were installed in [redacted], the monitoring equipment was not receiving or displaying camera video feed. Despite monitors being set up in the Postmaster's office, Postal Service management could not access the cameras or associated video feed. Finally, the CCTVs at the [redacted] S&DC were either not fully installed or did not have sufficient coverage of the EV charging stations.

According to Postal Service policy,[16] when a CCTV security system is used, it must cover all pedestrian and vehicle entries, including parking areas.

These issues occurred because these facilities were still in the process of implementing security measures, such as CCTVs to ensure adequate coverage of charging stations, during their transitions to becoming S&DCs.

Cameras provide physical security controls to allow supervisors or law enforcement to monitor and identify crime, abuse, or misuse of Postal Service assets, while also providing a deterrent to potential malicious actors. Thus, without proper CCTV coverage of all Postal Service assets, charging stations are at risk of misuse or tampering, which could disrupt vehicle charging and delay the delivery of mail.

During the audit, we contacted the Postal Inspection Service to discuss the CCTV issues identified during our site visits. They stated they are working with local management and contractors to establish video feed access at the [redacted] S&DC and ensure adequate camera coverage of the charging stations at the [redacted] S&DC.

Recommendation #4

We recommend the **Chief Postal Inspector,** in coordination with the **Vice President, Facilities**, determine if a closed-circuit television system is required to cover electric vehicle charging stations, and if so, install the system to allow for monitoring at the Sorting and Delivery center at [redacted].

Recommendation #5

We recommend the **Chief Postal Inspector**, in coordination with the **Vice President, Facilities** continue to work with local management to resume installation of the closed-circuit television system at the Sorting and Delivery Center in [redacted].

Recommendation #6

We recommend the **Chief Postal Inspector**, in coordination with the **Vice President, Facilities**, continue to work with local management to resume installation of the closed-circuit television system at the Sorting and Delivery Center in [redacted].

Postal Service Response

The Postal Service disagreed with this finding, but agreed with recommendations 4, 5, and 6.

Regarding the finding, management stated that the Postal Inspection Service has several sufficient physical security measures in place at the [redacted] S&DCs. Specifically, CCTV camera views of the EV charging stations are not considered a requirement by the S&DC policy.

Management agreed with recommendations 4, 5, and 6 and provided a target implementation date of April 30, 2026, for recommendations 4 and 6. Management implemented

16 RE-5 Building and Facility Security, Section 2-5.2.

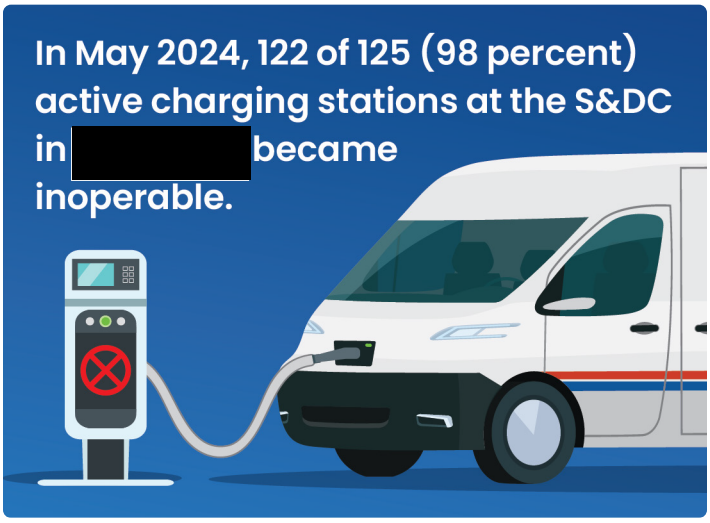
recommendation 5 prior to issuance of this report and requested that it be closed.

OIG Evaluation

Management's comments were responsive to recommendations 4, 5, and 6 and corrective actions should resolve the issues identified in the report. We reviewed evidence of CCTV installations at the [redacted], S&DC and agree that recommendation 5 can be closed upon issuance of this report.

Finding #3: Inadequate Contingency Planning

The Postal Service, as part of a coordinated approach with its National Preparedness Office, had options in place for when a natural disaster, power outage, or charging station nonfunctionally occurs, such as hot swaps of nonfunctional equipment, deployment of generators, and flexibility of not having to charge vehicles every day. However, the S&DCs we visited did not have these options documented in their contingency response plans to address potential EV charging station outages, such as those that occurred at the S&DC in [redacted], during 2024.



Specifically, in May 2024, 122 out of 125 (98 percent) active charging stations at the S&DC in [redacted] became inoperable. In addition, between May 2024 and July 2024, over 40 out of 125 (32 percent) active charging stations became inoperable at least 21 times.

According to policy,[17] the Postal Service is responsible for the development of plans for actions necessary to maintain itself as a viable part of the Federal government during any emergency that might occur. Preparedness planning within the Postal Service includes planning for domestic emergencies, such as conditions resulting from natural or human-caused disasters. These conditions may affect a single Postal Service facility or have a widespread effect on the entire Postal Service.

These plans were not documented at the local level because Postal Service Headquarters personnel considered contingency planning important, but not urgent. Without documented contingency operating plans, facilities run the risk of not being able to fulfill performance requirements due to lack of functioning EV delivery vehicles. Contingency planning would allow for Postal Service facilities to be better equipped to deal with potential EV charging issues and to deliver mail as scheduled.

Recommendation #7

We recommend **National Director of the Next Generation Delivery Program Office**, in coordination with the **National Director of the National Preparedness Office**, and the **Vice President, Delivery Operations** provide suggested guidance to the district level to update their contingency operations plans to account for the inoperability of charging stations.

Postal Service Response

The Postal Service disagreed with the details pertaining to this finding but agreed with the need to update existing contingency plans and recommendation 7.

Management stated that during the two power outages at the [redacted] there were no vehicles deployed there and disagrees that contingency planning should have been in place before vehicles were deployed to a location.

Management agreed to implement recommendation 7 and provided a target implementation date of December 15, 2025.

OIG Evaluation

Management's comments were responsive to recommendation 7 and corrective actions should resolve the issues identified in the report.

17 Administrative Support Manual 13 28 Emergency Preparedness, 281 Contingency Planning.

Appendices

Appendix A: Additional Information

Scope and Methodology

We conducted site work at the [redacted] S&DCs from October 16, 2024, through January 9, 2025. We judgmentally selected these locations to assess physical security of EV charging stations from each of the Postal Service's three vendors.

We also worked with a contractor to conduct 24 hardware, network, and firmware tests on charging stations from each of the three of the vendors.

To accomplish our objective, we:

- Hired a contractor to test one model from each of the three vendors for EVs and tested them in a lab environment.
- Obtained and reviewed physical security policies for facility security to gain an understanding of the environment and assess physical security controls.
- Interviewed Postal Service management to determine roles and responsibilities related to security and physical controls.
- Assessed third party and supply chain risk management documentation.
- Requested contingency plans for charging stations in the event of charging stations being inoperable.

We conducted this performance audit from August 2024 through June 2025 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 23, 2025, and included its comments where appropriate.

In planning and conducting the audit, we obtained an understanding of EV charging station internal control structure to help determine the nature, timing, and extent of our audit procedures. We reviewed the management controls for overseeing the program and mitigating associated risks. Additionally, we assessed the internal control components and underlying principles, and we determined that the following three components were significant to our audit objective: 1) control environment, 2) risk assessment, and 3) information and communication.

We developed audit work to ensure that we assessed these controls. Based on the work performed, we identified internal control deficiencies related to information and communication that were significant within the context of our objectives. Our recommendations, if implemented, should correct the weaknesses we identified.

We assessed the reliability of EV vendor and location data through performance testing. We determined that the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

Report Title	Objective	Report Number	Final Report Date	Monetary Impact
Fleet Modernization – Electric Vehicle Charging Stations Acquisition	Determine whether the Postal Service was effectively testing and monitoring the performance of, providing effective oversight over the contract for, and storage of, charging stations.	23-059-R24	12/29/2023	[redacted]
Next Generation Delivery Vehicles – Environmental Impact Statement	To 1) determine if the Postal Service's NGDV acquisition process and the related EIS complied with NEPA and 2) assess the reliability and reasonableness of the EIS and supporting analysis. As part of our audit work, we engaged a contractor to assist with evaluating the EIS's underlying assumptions, data, models (including those for total cost of ownership and environmental emissions), and conclusions.	22-107-R23	4/6/2023	NA
Vehicle Maintenance Facility Preparedness for Next Generation Delivery Vehicles	To assess the Postal Service's VMF preparedness plans to maintain the future fleet of Next Generation Delivery Vehicles.	22-045-R23	10/17/2022	NA
Delivery Vehicle Acquisition Strategy	To assess the Postal Service's acquisition strategy for delivery and collection vehicles.	19-002-R20	8/12/2020	NA

Appendix B: Management's Comments

UNITED STATES POSTAL SERVICE

May 29, 2025

VICTORIA SMITH
ACTING DIRECTOR, AUDIT SERVICES

SUBJECT: Management Response: *Security of Electric Vehicle Charging Stations (24-020)*

Thank you for providing the Postal Service with an opportunity to review and comment on the findings and recommendations contained in the draft audit report, *Security of Electric Vehicle Charging Stations (EVSE).*

It is important to note that this equipment is Commercial Off-The-Shelf (COTS) equipment, with tens of thousands of implementations (or more, depending on supplier and model) successfully operating around the world. The Postal Service does not specify nor manage software development processes or features that govern EVSE security protocols – they are provided as part of each supplier's COTS solution.

The audit team made several adjustments to the final audit report based on input and documentation from the Postal Service; however, there are several items that are still not correctly or accurately reflected in the final report.

Background:

In the Background section, the audit report references information received from one specific EVSE supplier in reference to the OIG's contracted security testing, but continues to inaccurately reflect and selectively misstate information received from that supplier. The audit team initially received hardware information from this supplier's international product support team, though this team has no working knowledge of the specific configuration parameters for the Postal Service's specific equipment set. The OIG later disregarded information from the second team they contacted from this supplier (this is the supplier team that works directly with the Postal Service) and stated that the information received from the supplier regarding configuration, security and other differences were "inconsistent" – when in fact, the second the team provided much more accurate information based on their ongoing contractual relationship with the Postal Service, and the day-to-day operational knowledge of the equipment set acquired and implemented by the Postal Service.

The report states that "*According to Vendor One, the firmware code and core components of the model tested are identical to the Postal Service's model.*" This is

Page 1

untrue, and has been documented by the supplier of the equipment as such. In a letter sent from the supplier to the audit lead on 4/18/2025, the supplier instead states: "***The OIG test unit is an older*** [redacted] ***version charger*** *and based on our records, had the firmware upgraded to the latest firmware version* [redacted] **This is NOT the same hardware as procured by the Postal Service. In addition, the firmware version is also not the same.** "*The current version core firmware the USPS chargers are on is* [redacted] *which is one version back from the OIG version.*" It further states: "*For all the USPS chargers the supplier "pre-commissions" them prior to shipment and they are placed into a "unique" grouping during setup configuration.* ***This grouping set up the unique features the USPS chargers have such as No Modbus communications and approved*** [redacted] ***whitelist integration***." The OIG test unit was linked to a different grouping in the supplier's cloud network, which applied different configuration parameters, and resulted in differences in the features available on the equipment. "*This connection and/or setup process to the standard supplier cloud network will auto update the firmware for "standard" off the shelf chargers and place the charger into the "standard" grouping.* **These features are "*NOT used for the USPS chargers*"**.

The audit team received all this information directly from the supplier, stating that the hardware is different, that the firmware is different, and that the cloud configuration settings are different. This was also covered by the Postal Service with the audit team –yet the final report makes it appear as if it the OIG tested the same equipment that is in use by the Postal Service. It is NOT the same equipment. There are some components that are the same, but the hardware model, the firmware version, and most importantly, the configuration tested is absolutely different and yields different results than if the actual USPS equipment had been tested. The audit team's own photos in the early draft reports visually show the differences in the hardware itself. The Postal Service provided a side-by-side comparison, and the audit team removed the photo of the equipment from the final report, but the report still incorrectly represents that the same hardware, firmware and configurations were tested, and they absolutely were not. This results in misleading results and obfuscation of known differences that yield substantively different security profiles, between the equipment the audit team tested and the equipment the Postal Service procured.

The report states, "*We did not verify that the configuration settings on the model testing mirrored the Postal Service's*" – this is the fundamental issue. As stated, both in documentation from the supplier, and again, by the Postal Service, even IF the two units compared (the OIG's test unit and a USPS production unit) had identical hardware, which they did **not**; and identical firmware, which they did **not**; the comparative testing would yield different results based on the configuration parameters for the respective EVSE. These configuration values have the single greatest impact on the security settings – it this is the area that the audit team expressly did not to verify or test. The audit report leaves the inference of more substantive findings of security risk than actually exist for the Postal Service EVSE, simply because the actual hardware/firmware/configuration that the Postal Service acquired and fielded is simply NOT what was tested.

Further, the audit report states, "Vendor One confirmed that the configuration settings would not negate the vulnerabilities identified during testing." This is entirely inaccurate, and disputed directly in the letter sent to the OIG from this supplier on April 18, 2025. First, there is one disclosed vulnerability the audit report references; however, it does NOT exist in the USPS configuration – which the audit team notes they did not test. Because the audit team tested a different more standard configuration, they have no data about this issue in the USPS configuration – but the USPS parameters render this vulnerability irrelevant. Second, there is another disclosed vulnerability; however, to access this vulnerability, a bad actor must have physical access to a charger and the unit must be unscrewed and opened. The attacker would need to reverse engineer the code. Even if all these things occurred, the scope is limited to only a single charger, and its net impact is to make that charger unable to dispense power. The OIG's contractor required more than three hours to perpetuate this attack within a controlled lab setting. There is no way to extend this attack beyond the initial charger. Further, the audit report also leaves out that the charger can still be accessed by the USPS and the supplier because it still stays available for a remote fix. Beyond this, a completely [redacted] is responsible for the [redacted] and the over-the-air updates. If an attacker were intent on preventing the USPS fleet from charging, there are many faster, much less complicated ways to accomplish that goal. Simply stated, this known vulnerability exists; it is limited to a single processor that limits scope to a single charger. Because of the physical access needed and complexity of effecting the attack, the probability of such an attack is extraordinarily low, has nominal impact at best, and is easy for the Postal Service to remediate.

Finding #1: EV Charging Station Vulnerabilities

The Postal Service disagrees with this finding.

Vendor One "*had the highest risk of disruption of service*." This is great news for the Postal Service, as we've just shown, the level of risk and impact of the known vulnerability is trivial at best. It took the OIG's contractor, a skilled technical test and research company, more than three hours in a lab setting to accomplish this disruption. To do the same in a secure, lighted, fenced, operational postal facility would be much more challenging. As noted, the probability is extremely low, and even if successful, the impact is to a single charging station.

"*We were able to reprogram the charging station because it* [redacted] *methods to verify firmware updates.*" This is also inaccurate. The [redacted] that was attacked does not have [redacted] but this is by design. Those features reside and are preserved on a [redacted] altogether, which effectively constrains the impact to the single unit. The audit report selectively leaves out this important detail. The very functionality that the audit report states is missing is what effectively constraints its scope and allows it to be "fixed" remotely if such an event should occur. As the supplier stated: "the issue exists. It's low probability, minor impact, and easy to address."

Vendor Two: the audit report describes a [redacted] vulnerability, which would require the attacker not only to use a specific [redacted] as well as a [redacted] to apply the attack through a service menu. The EVSE supplier has acknowledged the issue and will be addressing it; however, similar to the other noted issue, the attack requires physical access, and its impact is limited to a single charging station. So as before, low probability, low impact, and easy to resolve.

For the findings for both Vendor One and Vendor Two, the audit report over-extends and over-exaggerates the potential impact of these highly unlikely vulnerabilities to "even delay mail delivery." This is hyperbole at best. These are single station attacks that take hours to perpetuate. Every site has multiple hot spares for charging, so even if one was down, there are spares available. And most routes/vehicles will not require daily charging, so there is limited, if any impact from a missed day of charging. If this extremely unlikely event were to occur, operations would certainly have to adjust, but the likelihood of service impact is incredibly speculative and inflammatory.

Vendor Three's only issue was related to use for the [redacted] which was noted for all three suppliers, that the [redacted] used to initiate charging sessions could be [redacted] and suggesting that the [redacted] are not protected from unauthorized use.

What the report fully leaves out is that the [redacted] are assigned by vehicle, and retained as an accountable item with the vehicle keys, which must be checked in and out by each carrier/driver every day, with every usage. These protocols directly parallel those in place for the [redacted] gas-powered vehicles every day across the nation.

In order to [redacted] one of the [redacted] a bad actor would first need access to the accountable items, the check-in/check-out process for which is documented for every vehicle daily. Beyond access, that person would need the skill set and equipment to successfully [redacted] And finally, the bad actor would need to use the charging station to charge their vehicle when USPS carriers are not parked and using the EVSE spaces and equipment, typically when carriers are on the street between generally 9am-4pm. During this time, the parking lots are largely empty, so a non-USPS vehicle parked in and charging at a fleet charging space would be highly visible and easy to stop.

The other important issue that is not covered by the audit report is that the use of standard [redacted] is one of a small set of possible authentication methods enabled by COTS EVSE. One option is to leave the chargers "open" so that anyone could charge – a far greater security risk than with the [redacted] Other options include using [redacted] for authentication. This, however, would put personally identifiable information for every possible EV driver into scope and risk for security risk. Similarly, the Postal Service could continue development of potential use of the [redacted] as the method of authentication; however, this would put the whole USPS network into security scope and risk. The USPS' selected authentication method with [redacted] is not only the most cost-effective solution leveraging existing accountability procedures, but also provides the least security risk exposure of all

available options. Surely in its critique of this solution, the audit team is not advocating for other more expensive, more high-risk and less secure solutions? However, none of these options were assessed by the audit team; merely the current solution was criticized. One would think the selection of this option from available COTS solutions would be pertinent and recognized within the scope of a security audit, but was notably excluded here despite the prudent position taken by the Postal Service, and despite detailed coverage of this information by the Postal team.

Finding #2: Inadequate Physical Security of Charging Stations

Management disagrees with this finding.

The Postal Inspection Service has several physical security measures in place at the [redacted] S&DCs. The Postal Inspection Service does have sufficient physical security controls at the S&DCs in [redacted] CCTV camera views of the EV charging stations are not considered a requirement by the SDC policy.

Finding #3: Inadequate Contingency Planning

The Postal Service agrees with the need to update existing contingency plans, but disagrees with the details associated with this finding.

In this section, the audit report notes outages in May 2024 in [redacted] (122 of 125 stations) and (40 of 125 stations). The first event occurred during a national outage; the second was when the site was awaiting a firmware update which was resolved shortly after. All charging stations were restored to full service – though it is important to note that NO VEHICLES had yet been deployed to this site yet prior to either of these outages. While the Postal Service agrees that contingency planning is important, we disagree that contingency planning should have been in place before the vehicles were even deployed to this location. Both of the sets of issues referenced in the report were fully addressed prior even to the initiation of vehicle deployments. It seems an unfair criticism to rebuke the Postal Service for a lack of a contingency when it was months prior to even receiving the vehicles – much less experiencing a failure that actually had the potential to impact the vehicles.

The following are responses to each of the seven recommendations.

Recommendation 1:
We recommend that the **Chief Logistics and Infrastructure Officer and Executive Vice President**, work with Vendor One to remediate (or accept the risks associated with) the vulnerabilities identified with its charging stations.

Management Response/Action Plan:
Management **disagrees** with this recommendation, and accepts the nominal risk of this low-probability, low impact, easy-to-address issue.

Target Implementation Date: N/A

Responsible Official: N/A

Recommendation 2:
We recommend that the **Chief Logistics and Infrastructure Officer and Executive Vice President**, work with Vendor Two to remediate (or accept the risks associated with) the vulnerabilities identified with its charging stations.

Management Response/Action Plan:
Management **disagrees** with this recommendation, and accepts the nominal risk of this low-probability, low impact, easy-to-resolve issue.

Target Implementation Date: N/A

Responsible Official: N/A

Recommendation 3:
We recommend that the **Chief Logistics and Infrastructure Officer and Executive Vice President**, work with Vendor Three to remediate (or accept the risks associated with) the vulnerability identified with its charging stations.

Management Response/Action Plan:
Management **disagrees** with this recommendation, and accept the nominal risk of the low probability, low-impact issue.

Target Implementation Date: N/A

Responsible Official: N/A

Recommendation 4:
We recommend **the Chief Postal Inspector, in coordination with the Vice President, Facilities,** determine if a closed-circuit television system is required to cover electric vehicle charging stations, and if so, install the system to allow for monitoring at the Sorting and Delivery center at [redacted]

Management Response/Action Plan:
Management **agrees** with this recommendation.

The Inspection Service will coordinate with facilities to determine if a closed-circuit television system is required to cover the electric vehicle charging stations. If it is

Page 6

determined that there should be a CCTV system, one will be installed that allows for monitoring at the SDC in [redacted]

Target Implementation Date: 04/30/2026

Responsible Official:
Chief Postal Inspector, in coordination with the **Vice President, Facilities**

Recommendation 5:
We recommend the **Chief Postal Inspector, in coordination with the Vice President, Facilities** continue to work with local management to resume installation of the closed-circuit television system at the Sorting and Delivery Center in [redacted]

Management Response/Action Plan:
Management **agrees** with this recommendation.

The Inspection Service has implemented this recommendation prior to the issuance of the draft report. The postmaster's office now has a functioning camera and monitor system to view the video feed.

Target Implementation Date: 11/30/2025

Responsible Official:
Chief Postal Inspector, in coordination with the **Vice President, Facilities**

Recommendation 6:
We recommend the **Chief Postal Inspector, in coordination with the Vice President, Facilities,** continue to work with local management to resume installation of the closed-circuit television system at the Sorting and Delivery Center in [redacted]

Management Response/Action Plan:
Management **agrees** with this recommendation.

The Inspection Service will coordinate with Facilities and work with local management to resume the installation of closed-circuit television system at the SDC in [redacted]

Target Implementation Date: 04/30/2026

Responsible Official:
Chief Postal Inspector, in coordination with the **Vice President, Facilities**

Page 7

Recommendation 7:
We recommend National Director of the Next Generation Delivery Program Office, in coordination with the National Director of the National Preparedness Office, and the Vice President, Delivery Operations provide suggested guidance to the district level to update their contingency operations plans to account for the inoperability of charging stations.

Management Response/Action Plan:
Management **agrees** with this recommendation, to the extent that this work is already in process.

Target Implementation Date: 12/15/2025

Responsible Official:
Director of the Next Generation Delivery Program Office, in coordination with the National Director of the National Preparedness Office, and Vice President, Delivery Operations

Victoria K Stephen
for RONNIE J. JARRIEL
CHIEF LOGISTICS AND INFRASTRUCTURE OFFICER
AND EXECUTIVE VICE PRESIDENT

E-SIGNED by GARY.R BARKSDALE
on 2025-05-29 12:10:16 EDT
GARY BARKSDALE
CHIEF POSTAL INSPECTOR

E-SIGNED by JOHN.S MORGAN
on 2025-05-29 07:33:57 EDT
JOHN S. MORGAN
VICE PRESIDENT DELIVERY OPERATIONS

E-SIGNED by RAE.A HAIGHT
on 2025-05-29 09:05:30 EDT
RAE ANN HAIGHT
DIRECTOR OF OFFICE OF THE NATIONAL PREPAREDNESS

cc: *Corporate Audit & Response Management*

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

This document contains sensitive information that has been redacted for public release. These redactions were coordinated with USPS and agreed to by the OIG.