

**SAN BERNARDINO COUNTY  
AUDITOR-CONTROLLER/TREASURER/TAX COLLECTOR  
INTERNAL AUDITS DIVISION**

---



**FLEET MANAGEMENT DEPARTMENT:  
INFORMATION SYSTEMS SECURITY CONTROLS FOLLOW-UP  
AUDIT**

---

**BOARD OF SUPERVISORS**

---

**COL. PAUL COOK (RET.),**  
FIRST DISTRICT

**JESSE ARMENDAREZ**  
SECOND DISTRICT

**DAWN ROWE, CHAIRMAN**  
THIRD DISTRICT

**CURT HAGMAN**  
FOURTH DISTRICT

**JOE BACA, JR. VICE CHAIR**  
FIFTH DISTRICT

**ENSEN MASON CPA, CFA**  
AUDITOR-CONTROLLER/TREASURER/TAX COLLECTOR  
268 WEST HOSPITALITY LANE  
SAN BERNARDINO, CA 92415-0018  
(909) 382-3183

WEBSITE: [HTTP://WWW.SBCOUNTYATC.GOV](http://www.sbcountyatc.gov)  
FRAUD, WASTE, & ABUSE HOTLINE: (800) 547-9540



## ***Mission Statement***

*This office is committed to serving our customers by processing, safeguarding, and providing information regarding the finances and public records of the County. We perform these functions with integrity, independent judgment, and outstanding service. We are accurate, timely, courteous, innovative, and efficient because of our well-trained and accountable staff.*

---

## **Audit Team**

**Denise Mejico, CFE**

Chief Deputy Auditor

**Menaka Burkitt, CFE**

Internal Audits Manager

**Carmel Manela CIA, CFE**

Senior Supervising Accountant/Auditor

**Paulina Arias**

Accountant/Auditor

# **Fleet Management Department: Information Systems Security Controls Follow-up Audit**

<b>Audit Report Letter</b>	<b>1</b>
<b>Scope, Objective, and Methodology</b>	<b>3</b>
<b>Prior Audit Findings, Recommendations, and Current Status</b>	<b>4</b>





## San Bernardino County

### Auditor–Controller/Treasurer/Tax Collector

**Ensen Mason CPA, CFA**

*Auditor–Controller/Treasurer/Tax Collector*

**John Johnson**

*Assistant Auditor–Controller/Treasurer/Tax Collector*

**Diana Atkeson**

*Assistant Auditor–Controller/Treasurer/Tax Collector*

**Vanessa Doyle**

*Assistant Auditor–Controller/Treasurer/Tax Collector*

March 17, 2025

Mark McCullough, Director  
Fleet Management  
210 North Lena Road  
San Bernardino, CA 92415

RE: Information Systems Security Controls Follow-up Audit

We have completed a follow-up audit of the Fleet Management Department's (Department) Information Systems Security Controls for the period of January 1, 2024, through August 29, 2024. The objective of the audit was to determine if the recommendations for the findings in the Fleet Management Information Systems Security Controls Audit report dated June 13, 2023, have been implemented. We conducted our audit in accordance with the International Standards for the Professional Practice of Internal Auditing established by the Institute of Internal Auditors.


We have provided a status of the audit findings identified in the original audit report issued on June 13, 2023. Of the 2 recommendations from the original audit report, 1 has been implemented and 1 has been partially implemented.

We sent a draft report to the Department on January 30, 2025. The Department's responses to the current status of our recommendations are included in this report.

We would like to express our appreciation to the personnel at the Department who assisted and cooperated with us during this engagement.

Respectfully submitted,

Ensen Mason CPA, CFA  
Auditor-Controller/Treasurer/Tax Collector  
San Bernardino County

By:   
Denise Mejico, CFE  
Chief Deputy Auditor

Distribution of Audit Report:

Col. Paul Cook (Ret.), 1st District Supervisor  
Jesse Armendarez, 2nd District Supervisor  
Dawn Rowe, Chairman, 3rd District Supervisor  
Curt Hagman, 4th District Supervisor  
Joe Baca, Jr., Vice Chair, 5th District Supervisor  
Luther Snoke, Chief Executive Officer  
Grand Jury  
San Bernardino County Audit Committee

Date Report Distributed: 3/21/25

EM:DLM:PBA:jm

### Scope and Objective

Our audit examined the Department's Information Systems Security Controls for the period of January 1, 2024, through August 29, 2024.

The objective of this follow-up audit was to determine whether the Department implemented the recommendations contained in the prior audit report, *Fleet Management Information Systems Security Controls Audit*, issued on June 13, 2023.

### Methodology

In achieving the audit objective, the following audit procedures were performed, including but not limited to:

- Interviews of Department staff
- Reviews of Department policies and procedures related to information systems security controls
- Review of last audit
- Sampling and examination of password change reports, active user reports, and other system-generated reports

### **Prior Finding 1: Passwords were not changed periodically.**

The San Bernardino County Policy Manual Section 09-06 Computer System Data Security states that passwords will be periodically changed by the users in accordance with procedures established by the Office of Management Services.

The following conditions were identified during our testing:

- There were 19 out of 123 employees who had not changed their password in Faster Web within the last year.
- There were 18 out of 28 employees who had not changed their password in Faster Motor Pool within the last year.

The Department did not have a policy or procedure requiring passwords to be changed periodically. When policies and procedures are not established, the risk of unauthorized personnel gaining access to the Department's information systems and making unauthorized changes increases.

### **Recommendation:**

We recommend the Department develop, implement, and communicate procedures regarding password strength and change frequency requirements. Additionally, we recommend that passwords be periodically changed according to the established Department procedures.

### **Current Status: Implemented**

The Department follows San Bernardino County Policy Manual 09-06 – Computer System Data Security as it relates to passwords and has distributed an internal memo to staff requesting passwords to be changed annually in accordance with County Policy.

Furthermore, the Department ensures passwords are changed periodically by reviewing the staff's last password change date. A second reminder in October is sent to staff who have not updated their passwords. Finally, in November, the Department will inactivate user accounts for all staff who have not changed their passwords. These accounts can only be reactivated by authorized administrative personnel, and the system will require the password to be changed once staff attempts to login.

**Prior Finding 2: Access to information systems was not removed when employees terminated County employment.**

The San Bernardino County Policy Manual Section 09-06SP County Central Computer System Data Security states that County assets in the form of computer data must be protected from unauthorized disclosure, modification, and destruction. The County Central Computer System must be secure from outside intruders, and County employee access must be restricted to authorized limits.

The following conditions were identified during our testing:

- There were 2 out of 123 active accounts in Faster Web for which access was not removed when employees were terminated.
- There were 7 out of 28 active accounts in Faster Motor Pool for which access was not removed when employees were terminated.

The Department does not regularly review and compare active accounts to terminated employee listings. When terminated employees have active accounts in the Department information systems, the risk of unauthorized changes in the systems is increased.

**Recommendation:**

We recommend the Department develop, implement, and communicate procedures to perform documented reviews of active user accounts and compare them to terminated employee listings. Additionally, we recommend the Department periodically review active user accounts and compare them to terminated employee listings according to the established Department procedures.

**Current Status: Partially Implemented**

The Department has updated their policies and procedures and requires Form FLTM 061 ITD Onboarding and Separating Employees Checklist to be completed and filed in the employee's personnel file. The on/off-boarding checklist is used to record which systems the new hire was granted access to and, upon the employee's departure from the Department, to record the date in which access to such systems is removed.

The Department verifies, in two different instances, that access to accounts is restricted for the employees who depart from the County, or Department. The first



instance is at the time of termination, and the second instance is during the annual password update review process. The Department has reviewed and compared active accounts to terminated employee listings and all of the tested accounts were inactive.

However, when we tested 3 terminated employees whose access had been removed, there were 2 accounts in which access was not removed within a reasonable timeframe when terminated. One employee's access was removed 3 years after the termination date and another's access was removed 8 months after the termination date.

Additionally, the following conditions were identified when we tested 6 active user accounts:

- There were 2 out of 3 active user accounts in the Fuel View Active User list for which access was not removed when employees were terminated.
- There were 1 out of 3 active user accounts in the Faster Web Active User list for which access was not removed when employees were terminated.

### **Management's Response:**

Fleet acknowledges the audit findings and is committed to strengthening IT security by improving password management practices. To enhance password security and compliance, the department agrees with the findings and will implement the following measures:

- Onboarding and Offboarding Compliance: Fleet will communicate and provide training on completing Form FLTM 061 – ITD Onboarding and Separating Employees Checklist to ensure proper account management.
- Monthly Password Review: Fleet will conduct reviews of department user password changes (excluding actual passwords) to verify that updates are made in accordance with the new policy.
- Verify Access: The department will prevent terminated employees from accessing terminated accounts in FASTER and Fuel View by removing account holder access to terminated employees. This is done by the ITD embedded staff running a password access report and cross referencing the list with the offboarding forms provided by the Payroll Specialist. This is the same technical process that is used now; however, we are increasing the frequency. We are adding a monthly review in addition to the action that should happen in real time and annually.



These steps will reinforce Fleet's commitment to IT security and ensure compliance with established County policies.

**Auditor's Response:**

The Department's actions and planned actions will correct the deficiencies noted in the finding.