LA18-12

# STATE OF NEVADA

# Performance Audit

## Department of Public Safety
## Records, Communications and Compliance Division

## Information Security

## 2017

Legislative Auditor
Carson City, Nevada

# Audit Highlights

Highlights of performance audit report on the Department of Public Safety's Records, Communications and Compliance Division, Information Security issued on January 17, 2018. Legislative Auditor report # LA18-12.

## Background

The mission of the Department of Public Safety's (DPS) Records, Communications and Compliance Division (Division) is to support Nevada's criminal justice community and its citizens by providing complete, timely, and accurate information in a manner that balances the need for public safety and individuals' rights to privacy and ensures a positive customer service experience.

The Division has four office locations statewide with two in Carson City and two in Las Vegas. For fiscal year 2017, the Division was authorized 185 full-time equivalent employees statewide.

In the 2013 Legislative Session, the Division's IT staff were removed and consolidated with the Division of Enterprise Technology Services (EITS) within the Department of Administration. The Division relies on EITS for its information technology support.

In fiscal year 2016, the Division had expenditures of $24.9 million. The Division's primary funding source of $15.4 million comes from licenses and fees.

## Purpose of Audit

The purpose of our audit was to determine if the Division has adequate information security controls in place to protect the confidentiality, integrity, and availability of its information and information processing systems. Our audit focused on the systems and practices in place during fiscal year 2017.

## Audit Recommendations

This audit report contains 10 recommendations to improve the security of the Division's information systems. The Division accepted the 10 recommendations.

## Recommendation Status

The Division's 60-day plan for corrective action is due on April 12, 2018. In addition, the six-month report on the status of audit recommendations is due on October 12, 2018.

# Records, Communications and Compliance Division Information Security

## Department of Public Safety

## Summary

Weaknesses exist in the Division's information security controls. These weaknesses include not disabling and removing former employee network user accounts when they leave Division employment. In addition, some employees did not complete their annual security awareness training. Finally, the Division lacks documentation and review of user access to mission critical applications.

Other security-related controls need improvement. Weaknesses include the Division's lack of a disaster recovery plan, as well as a completed service level agreement with EITS to clarify the scope, quality, responsibilities, and backup requirements of its hosted systems.

## Key Findings

Weaknesses exist in managing the Division's network user accounts. Of the Division's 234 network user accounts, we identified 63 accounts of former employees whose network access had not been disabled or removed in a timely manner. Untimely disabling of former employees' network user accounts increases the risk that someone could gain unauthorized access to sensitive criminal justice information. (page 4)

Forty-one of the Division's 179 staff and vendors have not completed their annual security awareness training. State security standards require all state employees to have security awareness refresher training to ensure they stay aware of current security threats, as well as understanding their responsibility to keep state information confidential. (page 5)

The Division does not maintain a master list of authorized users or review system access privileges for several of its mission critical applications. Through these applications, the Division collects and stores sensitive criminal justice information. Without the proper documentation of authorized users and annual review of system access privileges, the Division would not have the ability to determine if current user access was appropriate. State security standards dictate system managers shall reevaluate system access privileges granted to all users annually. (page 5)

The Division does not have a disaster recovery plan. A disaster recovery plan ensures the prioritization of mission critical services for restoration in the event of an emergency. Without a current disaster recovery plan, there is a greater risk that some unforeseeable event or disaster could jeopardize access to sensitive criminal justice information contained in the Division's systems. Timely restoration of such mission critical services could be severely affected when this plan does not exist. For example, public safety could be impacted if DPS was unable to access the criminal history information contained in the Division's systems. (page 7)

A service level agreement is not in place between the Division and EITS. This agreement clearly states what an organization needs, and defines what is expected of a service provider. Without a completed and signed agreement between the Division and EITS, operations continue without a clear commitment in place to clarify the scope, quality, and responsibilities of each party. (page 9)

The Division does not have an agreement in place to communicate backup requirements of its systems hosted with EITS. Without the documentation an agreement provides, the Division is unable to ensure adequate backups are in place for its systems. Adequate backups are essential to ensuring recovery of information and the ability to provide support of critical business functions. We found backups were being performed by EITS, but without the Division's oversight. (page 9)

STATE OF NEVADA
LEGISLATIVE COUNSEL BUREAU
LEGISLATIVE BUILDING
401 S. CARSON STREET
CARSON CITY, NEVADA 89701-4747

RICK COMBS, *Director*
(775) 684-6800

LEGISLATIVE COMMISSION (775) 684-6800
JASON FRIERSON, *Assemblyman, Chairman*
Rick Combs, *Director, Secretary*

INTERIM FINANCE COMMITTEE (775) 684-6821
JOYCE WOODHOUSE, *Senator, Chair*
Mark Krmpotic, *Fiscal Analyst*
Cindy Jones, *Fiscal Analyst*

BRENDA J. ERDOES, *Legislative Counsel* (775) 684-6830
ROCKY COOPER, *Legislative Auditor* (775) 684-6815
SUSAN E. SCHOLLEY, *Research Director* (775) 684-6825

Legislative Commission
Legislative Building
Carson City, Nevada

This report contains the findings, conclusions, and recommendations from our performance audit of the Department of Public Safety's Records, Communications and Compliance Division, Information Security. This audit was conducted pursuant to the ongoing program of the Legislative Auditor as authorized by the Legislative Commission. The purpose of legislative audits is to improve state government by providing the Legislature, state officials, and Nevada citizens with independent and reliable information about the operations of state agencies, programs, activities, and functions.

This report includes 10 recommendations to improve the security of the Division's information systems. We are available to discuss these recommendations or any other items in the report with any legislative committees, individual legislators, or other state officials.

Respectfully submitted,

Rocky Cooper, CPA
Legislative Auditor

November 1, 2017
Carson City, Nevada

# Records, Communications and Compliance Division
# Information Security
# Table of Contents

# Introduction

## Background

The General Services Division was renamed to the Records, Communications and Compliance Division (Division) during the 2017 Legislative Session. The Division is one of eight divisions within the Department of Public Safety (DPS). The Division's mission is to support Nevada's criminal justice community and its citizens by providing complete, timely, and accurate information in a manner that balances the need for public safety and individuals' rights to privacy and ensures a positive customer service experience.

The Division has four office locations statewide with two in Carson City and two in Las Vegas. The Division was authorized for 185 full-time equivalent employees in fiscal year 2017.

In the 2013 Legislative Session, the Division's IT staff were removed and consolidated with the Division of Enterprise Technology Services (EITS) within the Department of Administration. The purpose of EITS is to provide information technology services and support to agencies located in Nevada so they can provide public services to Nevada citizens and visitors.

The Division currently consists of two bureaus: 1) the Communications Bureau, and 2) the Records Bureau. The two bureaus are organized as follows:

**Communications Bureau**

- Dispatch
- Warrants

**Records Bureau**

- Criminal History Repository
- Fiscal Unit
- Point of Contact Firearms Program
- Sex Offender Registry and Community Notification

- Nevada Criminal Justice Information System (NCJIS) Compliance Unit
- Civil Name Check
- Uniform Crime Reporting

DPS has an Information Security Officer to address the Federal Bureau of Investigation, Criminal Justice Information Services Security compliance. The Division employed an Information Security Officer in fiscal year 2016 to meet state security requirements. However, the Division relies on EITS for its information technology support.

Exhibit 1 shows a summary of the Division's two budget accounts. The Division's primary funding source of $15.4 million comes from licenses and fees. For fiscal year 2016, the Division's combined revenues and expenditures are reflected below.

**Revenues and Expenditures** **Exhibit 1**
**Fiscal Year 2016**

| | Amount |
|---|---|
| **Revenues** | |
| State Appropriations | $ 1,186,856 |
| Beginning Funds | 8,669,628 |
| Licenses and Fees | 15,385,711 |
| Other Revenues[1] | 8,304,485 |
| Transfer From Other State Agencies | 1,637,761 |
| **Total Revenues** | **$35,184,441** |
| **Expenditures** | |
| Personnel | $10,565,236 |
| Operating[2] | 834,708 |
| Equipment | 27,298 |
| Program Costs | 5,696,208 |
| Information Services | 3,638,433 |
| State Cost Allocations and Assessments | 4,112,449 |
| **Total Expenditures** | **$24,874,332** |
| Difference | $10,310,109 |
| Less: Reversion to General Fund | 100 |
| **Balance Forward to 2017** | **$10,310,009** |

Source: State accounting system.

(1) Other revenues include cost reimbursements.

(2) Operating costs include travel, buildings and grounds, and other operating expenditures.

## Scope and Objective

The scope of our audit included a review of the systems and practices in place during fiscal year 2017. Our audit objective was to:

- Determine if the Records, Communications and Compliance Division has adequate information security controls in place to protect the confidentiality, integrity, and availability of its information and information processing systems.

This audit is part of the ongoing program of the Legislative Auditor as authorized by the Legislative Commission, and was made pursuant to the provisions of NRS 218G.010 to 218G.350. The Legislative Auditor conducts audits as part of the Legislature's oversight responsibility for public programs. The purpose of legislative audits is to improve state government by providing the Legislature, state officials, and Nevada citizens with independent and reliable information about the operations of state agencies, programs, activities, and functions.

# Weaknesses Found in Managing Network Users

Weaknesses exist in managing the Records, Communications and Compliance Division's (Division) network users. These weaknesses include not disabling and removing former employee network user accounts when they leave Division employment. In addition, some employees did not complete their annual security awareness training. Finally, the Division lacks documentation and review of access to mission critical applications.

## Former Staff Had Current Network Access

Of the Division's 234 network user accounts, we identified 63 user accounts of former employees whose network access had not been disabled or removed in a timely manner. Thirteen of these accounts were over 3 years old. Fifty-six accounts were enabled until their passwords expired, at which point a user could simply reset their password and continue to access network resources. The remaining seven accounts were disabled; however, the Division did not ensure their timely removal. The authoritative technology standards published in the Federal Information System Controls Audit Manual (FISCAM) state that user accounts should be disabled or removed in a timely manner upon an employee's departure. Untimely disabling of former employees' network user accounts increases the risk that someone could gain unauthorized access to sensitive criminal justice information.

The Division's procedure for disabling network user accounts for employees terminating or transferring was not effective. The procedure utilized the Division's exit procedures form that served as a supervisory reminder of steps to complete when an employee leaves the Division. However, the Division did not have a follow-up procedure to ensure these accounts were disabled and removed. The Division indicated efforts are planned to add policy applicable to this area in the service level agreement with EITS.

After this omission was brought to the Division's attention, the network user accounts were reviewed and subsequently removed.

## Some Staff Did Not Complete Annual Security Awareness Training

Forty-one of the Division's 179 staff and vendors had not completed their annual security awareness training. Fifteen of the 41 were vendors and contractors with no evidence that security awareness training had been completed. State security standards require all state employees to have security awareness refresher training to ensure they stay aware of current security threats, as well as understanding their responsibility to keep state information confidential. Furthermore, state security standards require all consultants and contractors to attend an orientation program that introduces security awareness and informs them of information security policies and procedures. Without completing such training, there is a greater risk that employees will not properly protect the information and systems they use.

This situation arose as a result of confusion about which security awareness training staff should take. While the state's security awareness training is required annually, the Division must also comply with the Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy. This policy mandates all personnel with access to criminal justice information have CJIS compliant security awareness training biennially. This caused uncertainty concerning which training was required. Either type of security awareness training will meet the state requirement; however, one must be completed annually. The Division indicated all employees had taken the required training by January 2017, after the omission was brought to the Division's attention during the audit.

## System Access Privileges Were Not Reviewed

The Division does not maintain a master list of authorized users or review system access privileges for several mission critical applications. Through these applications, the Division collects and stores sensitive criminal justice information.

State security standards indicate a master user list of all users shall be maintained, kept secured and updated, reflecting all systems to which they have access. In addition, system managers shall reevaluate system access privileges granted to all

users annually, at a minimum. Furthermore, the Division is responsible for determining which users have access to its data based on the concept of least privilege. The concept of least privilege is based on the user's job function, and the minimum set of privileges required to perform that function, and the need to have separation of duties.

Through discussions with staff and management, we determined they were unaware of the requirements indicated in state security standards. Without a current list of authorized users and annual review of system access privileges, the Division did not have the ability to determine if current user access was appropriate. This lack of documentation and review increases the potential for unauthorized individuals to access sensitive criminal justice information.

## Recommendations

1. Revise the existing procedure to ensure the network user accounts of former employees are disabled and removed in a timely manner.
2. Create and maintain a complete list of all network user accounts and verify its accuracy on an annual basis.
3. Revise existing procedures to ensure all employees, vendors, and contractors receive annual security awareness training and maintain an updated list of completed trainings.
4. Create a master list of authorized user accounts to critical applications.
5. Develop a procedure to ensure system access privileges to critical applications are reviewed on an annual basis.

# Disaster Recovery Plan Not in Place

The Division does not have a disaster recovery plan. A disaster recovery plan ensures the prioritization of mission critical services for restoration in the event of an emergency. Information stored and processed on IT systems is vulnerable to degradation, accidental or intentional corruption or deletion, hardware and software failures, and natural or man-made disasters. To avoid disruption from such events, or to recover from them, a disaster recovery plan reduces the time needed to restore critical IT services, such as those that may impact public safety. For example, public safety could be impacted if DPS was unable to access the criminal history information contained in the Division's systems.

EITS hosts the Division's IT infrastructure and supports its information technology needs. In addition, EITS provides services to support the development and administration of state agencies' disaster recovery plans. However, state security standards indicate the Division as owner of the data is responsible for ensuring appropriate backup and recovery plans, procedures, retention schedules, and testing are accomplished and documented. During the course of the audit, we determined the Division could not provide a comprehensive list of its servers, including the business functions and applications of each system.

According to state security standards, the Division's Information Security Officer will oversee or be a member of a team. This officer or team member will be responsible for developing, maintaining, and testing, IT contingency, disaster recovery, and business resumption plans. The Division acknowledged it does not have a disaster recovery plan, and it did not have a staff member assigned to meet state security requirements until fiscal year 2016.

The Division had not assessed its critical information systems and components or identified its current disaster recovery capabilities. As a result of the audit, the Division is leading a departmental effort to update each Division's Critical Business Technology Assessment Program (CBTAP) information. CBTAP is a program that provides guidance and tools to assist in performing high-level business impact analysis of critical business functions. Performing this analysis will better prepare the Division to understand the impact of a disaster to its operations and know the risks in its current environment. Although the Division could not provide a comprehensive list of its servers, including business functions and applications of each system, they were able to provide a list of applications and their availability requirements as an EITS customer.

Without a current disaster recovery plan, there is a greater risk that some unforeseeable event or disaster could jeopardize access to sensitive criminal justice information contained in the Division's systems. Timely restoration of such mission critical services could be severely affected when this plan does not exist.

## Recommendations

6. Review and prioritize current critical information systems and components that support the Division's business functions on an annual basis.
7. Develop a disaster recovery plan for the Division's systems, applications, and data.

# Service Level Agreement Was Not Completed

A service level agreement (SLA) is not in place between the Division and EITS. This agreement clearly states what an organization needs, and defines what is expected of a service provider. The authoritative technology standards published by organizations such as the National Institute of Standards and Technology recommend an agreement should specify explicit definitions of both the organization's roles and responsibilities and the service provider's roles and responsibilities. Without a completed and signed agreement between the Division and EITS, operations continue without a clear commitment in place to clarify the scope, quality, and responsibilities of each party.

The Division is currently reviewing a draft document proposed by EITS. Former EITS leadership did not believe an SLA would be beneficial to the relationship between the two agencies and were reluctant to sign any documents that governed specific aspects of that association. Current EITS leadership is not opposed to an agreement and anticipates adopting an SLA.

## Backup Terms Were Not Clearly Defined

The Division does not have an agreement in place to communicate backup requirements of its systems hosted with EITS. Performing data backups is a service provided by EITS for the systems it hosts. The backup terms should be clearly defined in an agreement between the two parties. We found backups were being performed by EITS, but without the Division's oversight.

State security standards indicate the Division and host provider, EITS, must specify in a written agreement which agency will perform the backup of the applications and provide a schedule for doing it. EITS is responsible, at a minimum, for ensuring the backup and recovery of the operating systems.

Without the documentation an agreement provides, the Division is unable to ensure adequate backups are in place for its systems. In the absence of an agreement, there is an increased risk that sensitive criminal justice information may not be included in scheduled backups. Adequate backups are essential to ensuring recovery of information and the ability to provide support of critical business functions.

This situation was a result of the Division outsourcing its information technology needs to EITS and neglecting to complete an agreement that included backup requirements. Regardless, the Division as owner of the data is responsible to ensure schedules and procedures for adequate backups are in place.

## Recommendations

8. Complete a service level agreement between the Division and EITS that is reviewed on an annual basis.
9. Ensure the service level agreement defines backup requirements for the Division's systems.
10. Conduct periodic reviews to ensure schedules and procedures for adequate backups are in place.

# Appendix A
## Audit Methodology

To gain an understanding of the Records, Communications and Compliance Division, we interviewed Division management and staff. We also interviewed the EITS staff who support the Division to gain a broad understanding of the Division's IT resources and how they are organized, managed, and utilized. In addition, we reviewed generally accepted IT standards and guidelines from the State of Nevada, National Institute of Standards and Technology, and the Federal Information System Controls Audit Manual. We also reviewed financial information, budgets, legislative committee minutes, and other information describing the Division's activities. Furthermore, we documented and assessed internal controls over IT systems, users, and data resources.

We examined the server rooms housing the Division's equipment for physical security including adequate access controls, effective temperature monitoring controls, and after-hours automated notifications.

We requested the Division's disaster recovery plan to determine if it was current and recently tested with documented results. We also examined the Division's efforts at ensuring appropriate data backups of critical data were occurring.

To test controls limiting access to the Division's criminal justice information were in place, we examined user settings to determine if access to sensitive data was authorized and appropriate. We reviewed the controls over sensitive data in application and database environments to determine if sensitive data was being properly protected.

To determine if controls over desktop computer security were adequate, we tested all computers in use by the Division employees at each of the five locations to verify all desktop

computers had current operating system and anti-virus updates installed.

We determined if the Division's facility access card system that is used to grant access to restricted areas was properly administered. We reviewed configuration settings on all the Division's multifunction devices to determine if data was overwritten. We also verified wireless networks used by the Division were authorized and had proper security controls in place.

We examined user controls to ensure the timely disabling of network user accounts and completion of annual security awareness training. Lastly, we examined service agreements in place between the Division and EITS to determine if documented roles and responsibilities for services were defined between the two parties.

Our audit work was conducted from July 2016 to July 2017. Audit work was postponed during February and March so Audit Division IT staff could complete responsibilities related to the 2017 Legislative Session. We conducted this performance audit in accordance with generally accepted government auditing standards. 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

In accordance with NRS 218G.230, we furnished a copy of our preliminary report to the Records, Communications and Compliance Division. On October 17, 2017, we met with agency officials to discuss the results of the audit and requested a written response to the preliminary report. That response is contained in Appendix B, which begins on page 14.

Contributors to this report included:

Shirlee Eitel-Bingham, GSEC, NISP
Deputy Legislative Auditor

Sarah Gasporra, BBA
Deputy Legislative Auditor

S. Douglas Peterson, CISA, MPA
Information Systems Audit Supervisor

# Appendix B

## Response From the Records, Communications and Compliance Division

**Brian Sandoval**
*Governor*

Nevada Department of Public Safety

**James M. Wright**
*Director*

Records, Communications and Compliance Division

**Julie Butler**
*Division Administrator*

333 West Nye Lane, Suite 100
Carson City, Nevada 89706
Telephone (775) 684-6262 – Fax (775) 687-3289

October 24, 2017

Rocky Cooper, Legislative Auditor
Legislative Council Bureau
Legislative Building
401 S. Carson Street
Carson City, NV 89701-4747

Dear Mr. Cooper,

Thank you for the information provided in your audit report of October 10, 2017. The Records, Communications and Compliance Division (RCCD) appreciates all of the efforts of the Legislative Counsel Bureau in conducting this review and the work to complete it. Our response to your recommendations is provided below. We have also attached the "Division's Response to Audit Recommendations" indicating our acceptance of the recommendations.

**Recommendation 1: Revise the existing procedure to ensure the network user accounts of former employees are disabled and removed in a timely manner.**

*Response:* We accept this recommendation

We are adding steps to our off boarding procedure to ensure we have verification from EITS before we consider the employee/contractor account removed.

Specifically, we will take the response from EITS Desktop that the employee account was removed and add that document to the inactive employee/contractor file. We will verify the presence of that document in the employee/contractor file as a final step before moving the file to the inactive bin.

**Recommendation 2: Create and maintain a complete list of all network user accounts and verify its accuracy on an annual basis.**

*Response:* We accept this recommendation

Please see the response to recommendation 4.

**Recommendation 3: Revise existing procedures to ensure all employees, vendors, and contractors receive annual security awareness training and maintain an updated list of completed trainings.**

*Response:* We accept this recommendation

Our guidance to supervisors will be to have staff (including employees, vendors, and contractors) take CJIS Security Awareness Training every year, even though it is required for CJIS once every two years. We will use the reporting feature of the tool quarterly and provide reports to supervisors of employees that are overdue, as well as employees that are due in the next three months.

Each calendar year a report will be created of the staff members overdue by more than three months and the report will be provided to the Division Administrator.

**Recommendation 4: Create a master list of authorized user accounts to critical systems.**

*Response:* We accept this recommendation

We are in the process of creating the list of access rights (domain, shared folders, e-mail accounts, applications access, etc.) for each position in the division. We will create a list of the Position Control Numbers with access to each critical system, updating the actual employee name periodically. We consider domain/network access to be a critical system.

**Recommendation 5: Develop a procedure to ensure system access privileges to critical applications are reviewed on an annual basis.**

*Response:* We accept this recommendation

The access rights for each position in the division will be reviewed and updated annually, as well as any resulting changes to the lists of positions with access to each critical system. The lists of users for each critical system will be updated continuously as staff changes. The lists of actual users will be verified against the user accounts lists annually. The annual verification will be supervised by the Departmental ISO and the results formally reported to the Division Administrator.

**Recommendation 6: Review and prioritize current critical information systems and components that support the Division's business functions on an annual basis.**

*Response:* We accept this recommendation

The RCCD staff will meet once annually to assess and prioritize division business functions. The Departmental ISO will review and possibly update the list of information systems and components that support those business functions. The Departmental ISO will provide a formal list of the prioritized information systems and components to the Division Administrator and the EITS Agency IT Services Manager. If there is a response from EITS concerning the list of systems, components, or prioritization, the Departmental ISO will deliver that response to the Division Administrator.

**Recommendation 7: Develop a disaster recovery plan for the Division's systems, applications, and data.**

*Response:* We accept this recommendation

At the conclusion of the review of backup, data archiving and data replication, RCCD will document current DPS-EITS capabilities related to disaster recovery. RCCD will then formulate a Disaster Recovery Plan for the division's systems, applications, and data, using the risks identified in the Division's Continuity of Operations Plan, and incorporate only the abilities that currently exist. This plan will be in place by July 1, 2018.

In parallel with developing an initial Disaster Recovery Plan, RCCD will identify necessary enhancements to current capabilities and will incorporate the enhancements in the 2020/2021 budget request.

**Recommendation 8: Complete a service level agreement between the Division and EITS that is reviewed on an annual basis.**

*Response:* We accept this recommendation

DPS and EITS do have an SLA in place but it covers only server hosting.

DPS and EITS have been exchanging a draft of an inclusive Service Level Agreement (SLA) for about a year, and the language continues to get better with each iteration. So that an ideal agreement doesn't become the enemy of a basic functioning agreement, DPS is committed to having a signed agreement in place by November 30, 2017. The agreement will incorporate all the SLA items referenced in the recommendations and responses in this document either in the initial version of the SLA or the first quarterly revision.

In addition to being modified as-needed, the SLA will be reviewed on an annual basis. The review will include how well both parties kept to the terms of the agreement, whether there were shortcomings in service that impacted DPS business (regardless of whether the service provided was within the terms of the SLA), and how improvements in process or communication could enhance EITS ability to render service, or improve the value of the service to DPS. The review period will be defined and short, with both parties agreeing to changes to the SLA at the end of the period.

**Recommendation 9: Ensure the service level agreement defines backup requirements for the Division's systems.**

*Response:* We accept this recommendation

RCCD is currently documenting the current status of data and system backup, data archive, and data replication, in order to understand the complete picture of data recovery options using current resources. The Departmental ISO will present the results to the Division Administrator. Working with EITS, RCCD will determine immediate improvements to the backup and archive schedule, communicate those changes to EITS, and incorporate the new backup schedule in the DPS – EITS Service Level Agreement.

Prior to the next legislative session, RCCD will determine optimal levels of data and system backup, data archive, and data replication, work with EITS to determine the magnitude of the budget enhancement required to incorporate the changes, and include it in the budget request for 2020/2021.

**Recommendation 10: Conduct periodic reviews to ensure schedules and procedures for adequate backups are in place.**

*Response:* We accept this recommendation

RCCD will incorporate into the DPS – EITS SLA a requirement that EITS will, within one business day, report to DPS any issues, system failures, failed restoration requests, or disruptions, affecting DPS, related to ongoing backups, data archiving, or data replication.

Once per calendar quarter, the DPS Departmental ISO will verify with EITS the backup schedule for data and systems, data archiving, and data replication. EITS will provide evidence of a successful restore request from the prior 90 days. Lacking such an event, the Departmental ISO will request the restore of an arbitrary user folder, system element, or data table. The restore data will be inspected (with EITS assistance, if necessary) to determine the success of the restore operation.

RCCD will annually review the schedule for backup, archive, and data replication for necessity and sufficiency. RCCD will also review the record of data loss, recovery, and the impact on the business related to recovery

failures and/or prolonged recovery times. The results of the review will provide guidance for system improvement recommendations, if any.

Thank you again for the opportunity to review, identify, and address areas in which RCCD can improve internal processes that support our public safety mission.

Sincerely,

Julie Butler

Julie Butler, Administrator
Records Communications and Compliance Division
Nevada Department of Public Safety

# Records, Communications and Compliance Division's Response to Audit Recommendations

| | Recommendations | Accepted | Rejected |
|---|---|---|---|
| 1. | Revise the existing procedure to ensure the network user accounts of former employees are disabled and removed in a timely manner | X | |
| 2. | Create and maintain a complete list of all network user accounts and verify its accuracy on an annual basis | X | |
| 3. | Revise existing procedures to ensure all employees, vendors, and contractors receive annual security awareness training and maintain an updated list of completed trainings | X | |
| 4. | Create a master list of authorized user accounts to critical applications | X | |
| 5. | Develop a procedure to ensure system access privileges to critical applications are reviewed on an annual basis | X | |
| 6. | Review and prioritize current critical information systems and components that support the Division's business functions on an annual basis | X | |
| 7. | Develop a disaster recovery plan for the Division's systems, applications, and data | X | |
| 8. | Complete a service level agreement between the Division and EITS that is reviewed on an annual basis | X | |
| 9. | Ensure the service level agreement defines backup requirements for the Division's systems | X | |
| 10. | Conduct periodic reviews to ensure schedules and procedures for adequate backups are in place | X | |
| | TOTALS | 10 | |