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)