Audit Department

500 S Grand Central Pkwy Ste 5006 • PO Box 551120 • Las Vegas NV 89155-1120
(702) 455-3269 • Fax (702) 455-3893

Angela M. Darragh, CPA, CFE, CISA, Director

July 2, 2015

Mr. Don Burnette
Clark County Manager
500 South Grand Central Parkway, 6th Floor
Las Vegas, Nevada 89106

Dear Mr. Burnette:

We recently completed an audit of the Special Public Defender JustWare application. The audit was conducted in accordance with our annual audit plan and covers the period from January 1, 2014, to July 31, 2014. The last day of fieldwork was March 18, 2015. The objective of this audit was to determine whether adequate controls are in place to protect the integrity, confidentiality, and availability of information accessed through JustWare.

We found that controls to protect the integrity, confidentiality, and availability of information accessed through JustWare can be improved. We found areas that leave the data at risk, including the following:

- Generic user accounts.
- Default installation accounts.
- Delays in disabling network access for terminated employees. Vendors allowed excessive access with add, modify, and delete access to data.
- Information Technology personnel who no longer need access.
- Lack of risk assessments to identify threats.
- Inadequate disaster recovery and business continuity planning and testing.

A draft report was provided to the Special Public Defender for comment, and his response is included.

We appreciate the cooperation and assistance provided by the staff of the Special Public Defender.

Sincerely,

Angela M. Darragh

Angela M. Darragh, CPA
Audit Director

BOARD OF COUNTY COMMISSIONERS
STEVE SISOLAK, Chair • LARRY BROWN, Vice Chair
SUSAN BRAGER • TOM COLLINS • CHRIS GIUNCHIGLIANI • MARY BETH SCOW • LAWRENCE WEEKLY
DON BURNETTE, County Manager

AUDIT DEPARTMENT

Audit Report

Special Public Defender JustWare Application

July 2015

Angela M. Darragh, CPA, CISA, CFE
Audit Director

AUDIT COMMITTEE:
Commissioner Steve Sisolak
Commissioner Chris Giunchigliani
Commissioner Lawrence Weekly

TABLE OF CONTENTS

BACKGROUND 1

OBJECTIVES, SCOPE, AND METHODOLOGY 2

RESULTS IN BRIEF 3

DETAILED RESULTS 3

- **Access Not Necessary for Job Duties (HIGH)** 3
- **Default User Accounts Not Eliminated After Installation in 2009 (HIGH)** 4
- **Vendor Has System Account Password and Other Excessive Access (MEDIUM)** 4
- **No Risk Assessment Completed for the Application (MEDIUM)** 5
- **Disaster Recovery and Business Continuity Plan Is Not in Place (MEDIUM)** 6
- **Current Version of JustWare Not Installed (LOW)** 6

MANAGEMENT RESPONSE 7

BACKGROUND

The Special Public Defender's Office was created and authorized by the Board of County Commissioners on March 4, 1997. The office is comprised of two divisions: Criminal Defense and Family Defense.

The Criminal Defense Division is assigned murder cases by the courts when there is a conflict with the Public Defender's Office. In those cases where the death penalty is sought, the Special Public Defender's Office provides mitigation and investigation services. The Office may also retain expert testimony in the course of the defense. The Special Public Defender's Office also has an appellate division which represents clients on appeal before the Nevada Supreme Court, the United States Supreme Court, and the Ninth Circuit of Appeals.

The Family Defense Division provides legal representation to parents who are at risk of having their parental rights terminated. Family cases are also assigned by the Hearing Master or Family Court. Attorneys and social workers form a team to find referrals to appropriate social services and to reunite families under the court's supervision.

The Special Public Defender's Office implemented JustWare, a case management system, in May of 2009 and is operating version 5.9.20. The system is capable of maintaining detailed case data and notes, reporting (standard and adhoc), data sharing, task management, notifications, document automation, and financial information. The financial administration module of the system is not utilized. Clark County entered into a maintenance agreement with New Dawn Technologies to maintain the software that includes upgrades. The purchase of the software and recurring support agreement are shared with the Office of Appointed Counsel and Information Technology. The initial shared contract cost of the system was $110,187 for installation services and licenses. For the period December 1, 2014, to November 30, 2015, total shared costs amount to $118,018. JustWare Criminal Statistics report shows a total of 60 cases, unaudited, processed by the Criminal Division for the audit period. JustWare FPD Stats report shows 544 cases opened and 484 cases closed, unaudited, by the Family Division for the audit period.

The vendor accesses the software through Bomgar, an application that allows remote viewing of a shared display. Changes to the software are tracked through Clark County's Information Technology

department change management system. The Clark County Information Technology department manages the application backup and recovery processes.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objective of this audit is to determine whether adequate controls are in place to protect the integrity, confidentiality, and availability of information accessed through JustWare.

Our scope includes the period from January 1, 2014, to July 31, 2014. Our last day of fieldwork was March 18, 2015.

In order to obtain an understanding of the operating and control environment for JustWare, we met with Special Public Defender staff of the Criminal and Family Division and the administrative assistant who administers the JustWare application. We also met with Information Technology staff. We performed walkthroughs of the JustWare application processes as utilized by Special Public Defender office and reviewed report reconciliations. We then examined all user access reports for the application and database and compared these to the County's Human Resource system to determine whether users were active employees. We then reviewed all JustWare access to determine if access appeared appropriate based on the user's job. We reviewed the application risk assessment, security violations logs, backups, data recovery testing, disaster recovery plans, and business continuity plans. We also tested three monthly reports of case data by reconciling to JustWare reports.

Our review included an assessment of internal controls in the audited area. Any significant findings related to internal control are included in the detailed results. The last day of fieldwork was January 20, 2015.

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 objectives.

RESULTS IN BRIEF

Controls to protect the integrity, confidentiality, and availability of information accessed through JustWare can be improved. We found areas that leave the data at risk, including the following:

- Generic user accounts.
- Default installation accounts.
- Delays in disabling network access for terminated employees. Vendors allowed excessive access with add, modify, and delete access to data.
- Information Technology personnel who no longer need access.
- Lack of risk assessments to identify threats.
- Inadequate disaster recovery and business continuity planning and testing.

Each finding includes a ranking of risk based on the risk assessment that takes into consideration the circumstances of the current condition including compensating controls and the potential impact on reputation and customer confidence, safety and health, finances, productivity, and the possibility of fines or legal penalties.

DETAILED RESULTS

Access Not Necessary for Job Duties (HIGH)

We examined user access rights and compared rights to job functions at the application and database level and found the following exceptions:

- Five Information Technology personnel with application access that also allows view, insert, modify, and delete functions to data, which is not necessary for their job duties.
- 10 separated employees continued to have network access for up to 1,855 days after separation from the County.
- One active database user account for Information Technology staff that is no longer needed.

User account management is important to protect the integrity and confidentiality of data. Accounts should be deactivated immediately upon an employee's separation from employment to prevent intentional misuse of the account. Further, Clark County Technology Directive 1, Information Technology Security Policy, section IV.B

requires users to be granted the minimum necessary access to perform their job duties. Providing users the least amount of access necessary protects against intentional or unintentional misuse or modification of data.

Recommendation

1. Modify access for Information Technology personnel so that they do not have the ability to add, change, or delete data.
2. Deactivate network access for individuals identified as no longer County employees immediately upon separation from employment or change in job duties.
3. Implement a policy and procedure to periodically review all user access.

Default User Accounts Not Eliminated After Installation in 2009 (HIGH)

Six default system accounts were never removed from the system after the successful installation of JustWare in 2009. Logins of this type are generally deleted or deactivated during system implementation. These default accounts are a risk, as passwords are often commonly known or available on the internet. An individual who is able to gain access to the network can easily compromise these accounts to gain access to confidential data. Further, according to the SANS Institute (an international security information and certification resource), hackers are developing worms that automatically search for systems with default usernames and passwords.

Recommendation

1. Eliminate default accounts.

Vendor Has System Account Password and Other Excessive Access (MEDIUM)

The JustWare application has a system user account that is needed by the application to run processes. The vendor has the password and could potentially access and corrupt the application processes using this system account. The password was not changed by Information Technology when the system was installed in 2009.

The vendor also has two database user accounts with the SuperUser profile and one active production user account without an assigned security profile. None of these accounts have access to the network. We confirmed with the vendor that one database user is no longer on the vendor service team. SuperUser profile allows view, insert,

update, and delete for many critical production functions, including but not limited to business rules and case data. Login through the production application without an assigned profile will not allow access to data and functions.

Data is at risk if the vendor should gain access to the network through some other means. We believe that leaving the door open on the production application or database could compromise the integrity or availability of data. In order to protect data, vendors should only be allowed access to the test environment. The JustWare vendor assists clients through remote access and must gain permission from the client if it is necessary to troubleshoot the production environment. Therefore, having user account access on the production application or database is not necessary.

Recommendation

1. Change and safeguard the system user account password.
2. Allow vendors access to only the test environment through user accounts.
3. Eliminate all vendor named user accounts on the production application and database. User accounts in the test environment should only be activated when service is needed.

No Risk Assessment Completed for the Application (MEDIUM)

A risk assessment was not done to identify security risks and threats needing corrective action. Clark County Technology Directive 1, Information Technology Security Policy, section IV.A.1, requires that risk assessments be completed for applications that create, collect, process, store, or transmit data or information that is considered confidential by federal and/or state statutes. The JustWare application includes confidential data, such as information on child abuse and neglect covered under NRS432B and victims of sexual assaults under NRS 200.3771. Nevada Rules of Professional Conduct, Rule 1.6 also requires that lawyers not reveal information relating to representation of a client unless the client gives informed consent with certain exceptions. Exceptions to revealing information includes, but is not limited to, complying with other laws such as public record laws or a court order.

Recommendation

1. Complete a risk assessment for the JustWare application.

Disaster Recovery and Business Continuity Plan Is Not in Place (MEDIUM)

A disaster recovery and business continuity plan is not in place for JustWare. Clark County Technology Directive 1, Information Technology Security Policy, section IV.O, requires that a plan be in place to mitigate the various vulnerabilities to County computing systems and networks and to ensure the availability and integrity of data and continuity of operations in the result of a system failure. Procedures are also necessary to resume normal operations once the system is recovered. Generally, plans include testing to ensure data can be recovered from backups in the event of an outage or failure. We found backups for JustWare are not tested to ensure data is recoverable.

Recommendation

1. Complete a disaster recovery and business continuity plan.
2. Test backups on a regular basis.

Current Version of JustWare Not Installed (LOW)

The most current version of JustWare is not installed. The operating version 5.9.20 was released in June 2014, with the production environment upgraded July 14, 2014. The current version, version 5.10.34, was released December 12, 2014. The support agreement includes providing upgrades. The current version will allow remote access of calendars with mobile devices and correct processing errors noted by the vendor. The Special Public Defender's Office is experiencing inefficiencies, as current events and meetings that need to be tracked are entered into the JustWare calendar and into various other calendars for viewing away from the office. Staff in the Special Public Defender's Office relies on calendaring functions to meet court requirements. The current version will also address system errors, such as hyperlink issues within the docket session, updated SQL views, miscalculated start date of events, notes being overwritten, and document changes not saved when a case is refreshed.

Recommendation

1. Request Information Technology install the current version of JustWare.

SPECIAL PUBLIC DEFENDER
330 SOUTH THIRD ST., STE. 800
LAS VEGAS NV 89155
702-455-0210, FAX 455-6273

MEMORANDUM

DATE: June 19, 2015

TO: ANGELA M. DARRAGH, AUDIT DIRECTOR
AUDIT DEPARTMENT

FROM: DAVID M. SCHIECK

SUBJECT: JUSTWARE APPLICATION AUDIT

MANAGEMENT RESPONSE & ACTION PLAN

1. ACCESS NOT NECESSARY FOR JOB DUTIES

1. We agree that IT should modify access for their personnel so that they do not have the ability to add, change or delete data. We will follow up with IT Help Desk/IT App Platforms JAVA/Other to verify this has been accomplished. 2. We agree that employee network access should be deactivated timely upon separation from employment. We will provide IT with the Delete Account form within 24 hours of an employee's last day. 3. We agree that a policy should be in place to periodically review all user access. We will commence a quarterly review of user access with IT App Platfomrs JAVA/Other.

2. DEFAULT USER ACCOUNTS NOT ELIMINATED AFTER INSTALLATION

1. We agree that IT should eliminate the default accounts. We will follow up with IT App Platforms JAVA/Other to verify that same has been done.

3. VENDOR HAS SYSTEM ACCOUNT PASSWORD AND OTHER EXCESSIVE ACCESS

1. We agree that the system user account password should be changed by IT. We will follow up with IT Infrastructure/IT App Platforms JAVA/Other to verify same has been

done. 2. We feel the vendor should have access to the production database only through Bomgar for remote viewing of a shared display upon request by SPD for specific issues which are user specific as opposed to system wide issue. If system wide, then Vendor will have access to test environment. The test environment is currently only on one SPD Administrator computer. 3. We agree that the vendor should not have access to the database until IT has approved through proper channels in place, and that user accounts in the test environment should only be activated when service is needed. We will follow up with IT App Platforms JAVA/Other regarding this issue.

4. NO RISK ASSESSMENT COMPLETED FOR THE APPLICATION

1. We agree that a risk assessment needs to be completed by IT. We will work with Mike Smith to complete the assessment

5. DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN IS NOT IN PLACE

1. We agree a disaster recovery and business continuity plan should be in place. Randy Pike, Asst. SPD will be attending training and will prepare the COOP and we will provide it to the County. 2. We agree IT should conduct test backups on a regular basis. We will follow up with IT Infrastructure that they are conducting the regular backups on a quarterly basis

6. [SIC]

7. CURRENT VERSION OF JUSTWARE NOT INSTALLED

1. We agree that the latest version of JW should be installed. Notice was received on 6/3 that version 5.11.1.0 is the current version. We will forward these emails to IT (via Elmer Belmonte) when we receive them and request that the current version be pushed to the test environment and then after testing, the current version will be pushed to the end users