SOLANO COUNTY GRAND JURY

2019-2020

County System Inventory, Security, Backup and Recovery

County System Inventory, Security, Backup and Recovery

Solano County Grand Jury 2019-2020

I. SUMMARY

Technology is evolving rapidly and is an essential tool in the effective operation of Solano County government. Implementation of appropriate technology strategies is key to enhancing efficiency, reducing cost, and using information to provide the residents of Solano County with better customer service.

The Grand Jury completed a targeted review of the processes and procedures relating to the County's system inventory, security, backup and recovery activities. Interviews, tours and documentary reviews were conducted to evaluate the key controls and activities relating to these functions.

In its review, the Grand Jury found Department of Information Technology (DoIT) senior staff knowledgeable of technology industry standards, equipment, and infrastructure. It determined that DoIT has adequate policies and procedures with the necessary controls to effectively manage the County's computer and networking infrastructure and mitigate the County's technology risks. DoIT has developed and maintains a Disaster Recovery Plan, although DoIT staff disclosed that the plan needs some improvement. An aspect of the plan pertaining to power outage recovery is robust and has been tested. However, other areas have not been explicitly and thoroughly outlined and tested and are under review.

II. INTRODUCTION

DoIT provided an information sheet to the Grand Jury, which included new organizational reporting lines. The document indicated DoIT develops, implements and supports computing and communications technologies. It also provides technical services in support of the County's operations. DoIT carries out these responsibilities through a variety of divisions within the department, including one solely focused on information security.

In the last year, Solano County hired a new Chief Information Officer (CIO), who serves as the head of DoIT. This new CIO has instituted organizational changes in the department filling vacancies and adjusting some of the departmental lines of responsibility. The CIO also hired a Chief Technology Officer (CTO) to advise on future technology issues and possibilities as well as serve as the assistant department head.

The Solano County 2019-20 fiscal year (FY) recommended budget (approximately $26.3 million) outlined six priorities that establish fundamental areas key to enabling operational efficiencies. Two of these fall within the scope of this review: 1) Disaster Recovery & Business Continuity and 2) System & Data Security and Compliance. DoIT presented information to the Solano County Board of Supervisors regarding cyber security threats. The types of threats facing county governments today include ransomware, phishing emails, and the hacking of system

infrastructure. This, coupled with recent earthquakes, wildfires and power shutdowns, has highlighted the need to adequately address and mitigate these potential business interruption events.

With these facts in mind, the Grand Jury chose to conduct a targeted review of the County's system inventory, security, backup and recovery activities. The objective was to evaluate the effectiveness of the key controls, processes and procedures relating to these functions.

III. METHODOLOGY

Techniques used in deriving facts include:

- Interviews and Discussions with DoIT subject matter experts
- Tours of two Data Center locations
- Reviews of the following data, code, articles, and documents:
    - DoIT organizational chart
    - DoIT presentation to County Board of Supervisors
    - FY 2019-20 County Recommended Budget section on DoIT
    - Solano County Disaster Recovery Plan (DRP)
    - Internet and Newspaper articles
    - California Government Code, §6270.5
- Examinations of the following documents:
    - Enterprise System Catalog on July 12, 2019 and December 21, 2019
    - DoIT Acceptable Use Policy
    - DoIT Power Outage Checklist
    - Solano County Backup General Information
    - Tape Drive, Data Cartridge and Tape Library Data Sheets

IV. STATEMENT OF FACTS

A. Enterprise System Catalog

Senate Bill No. 272 amended the California Public Records Act on October 15, 2015. It added Government Code section 6270.5 mandating all local agencies publish a catalog of enterprise systems[1] by July 1, 2016. Review of the County's website on July 12, 2019 found that the County initially complied with the code by creating a catalog and posting it on its website accessible to the public. However, the downloaded file reflected a date of July 1, 2016, raising a concern with the completion of annual updates. Through interviews and further research, it was determined that the annual reviews have been completed but the updated files were not posted on the County's website. A copy of the most recent review completed in March 2019 was obtained. Upon notification, DoIT personnel took immediate corrective action and posted the most current file. Posting to the website was verified on December 21, 2019.

[1] "Enterprise system" means a software application or computer system that collects, stores, exchanges, and analyzes information that the agency uses that is both of the following: A) A multidepartmental system or a system that contains information collected about the public, and B) A system of record.

B. System and Data Security and Stability

A guiding principle of DoIT is to ensure County systems are safe, stable and secure, and will provide an integration mechanism to streamline business practices. This is reflected in the department's budget request for FY 2019-20. Many ongoing and planned projects seek to meet this principle.

County administration has directed DoIT to undertake a project to replace the aging Solano County Integrated Property Management System (SCIPS) with a new County Assessment and Taxation System (CATS). This system has been highlighted as a critically important system, and thus essentially "too big to fail". This project requires DoIT to work closely with County stakeholders (County Treasurer-Tax Collector-County Clerk, Assessor Recorder, Auditor-Controller, and software vendor) to ensure overall implementation success.

The 2017-18 Solano County Grand Jury issued a Finding and Recommendation regarding the replacement project in their report entitled "Property Tax Assessment & Payment Processing Review." The Board of Supervisors approved a $10 million reserve for the project on April 4, 2017. Current review of the Significant Challenges and Accomplishments comments in the FY 2019-20 Recommended County Budget indicates that the initial kickoff workshop began on February 25, 2019 officially starting the project. Phase 0 (Data Migration) of this project is estimated to take 12 months to complete and will be the focus of work in FY 2019-20. This phase will involve significant technical staff involvement performing data migration and validation activities as well as building an archive system for historical data. DoIT provided this Grand Jury with a copy of the current Project Plan defining the 13 phases and applicable timelines. Project completion is currently targeted for July 31, 2023.

At a County Board of Supervisor's meeting on October 1, 2019, DoIT personnel made a presentation recommending adopting a resolution to participate in recognizing October 2019 as National Cybersecurity Awareness Month. The three-fold theme and key message were to:

- Own IT

  Understand your digital profile – understand the devices and application you use everyday.

- Secure IT

  Secure your digital profile – learning about security features available on the equipment and software you use.

- Protect IT

  Maintain your digital profile – be familiar with and routinely check privacy settings to help protect your privacy and limit cybercrimes.

The presentation highlighted the following type and volume of recently encountered cyber security attacks against the County's network infrastructure. These attacks were all effectively blocked by DoIT's use of industry standard intrusion detection and mitigation tools. Defensive

strategies outlined in the presentation include continuing investment in new security technologies and educating County personnel on recognizing cyber threats.

Cybersecurity Attacks towards Solano County
Data For August 2019

Type of Cyber Security Attacks	Attack Count - Blocked
Network Attacks from the Internet	**21,288**
Malware Attacks	**19**
Email Viruses	**1,732**
Spam Emails	**47,235**

C. System and Data Backup

All enterprise data systems managed by DoIT are backed up on a regularly scheduled basis. Generally speaking, that includes all user generated files, such as Word documents and Excel spreadsheets, stored on file servers as well as the files in database management systems not directly created by system users. In interviews with key DoIT staff, the Grand Jury was advised that users are encouraged to avoid storing files of significant business value on their County issued personal computer equipment. Such files are not backed up by any of the processes executed by DoIT. A failure of a user's PC could result in the permanent loss of any data on that PC.

The backup of enterprise data systems is accomplished in three phases.

1) A full and complete backup of all files is taken annually in December, kept on-site on readily accessible hard disk storage for 35 days, after which it is migrated to tape for off-site storage for seven years.
2) A full and complete backup of all files is taken monthly, kept on-site on readily accessible hard disk storage for 35 days, after which it is migrated to tape for off-site storage for two years.
3) A cumulative incremental backup of files created or changed since the last full backup is taken daily, kept on-site on readily accessible hard disk storage for 35 days, after which it is purged.

Database backups are accomplished in a correspondingly similar fashion. The only difference is that daily cumulative incremental backups are retained for 70 days instead of 35 days before being purged, and the full backups are retained on-site for 70 days before being migrated off-site.

According to DoIT staff interviewed, there is no known need to retain any file backups beyond the standard seven-year maximum retention period established by the department. All tapes

returned from off-site storage at the conclusion of their respective retention periods are securely and completely wiped clean of all data and returned to the tape library as scratch tapes for subsequent use. Tapes that are damaged or have reached the end of their useful life are securely and completely wiped clean before disposal.

The tape library subsystem currently employed by DoIT is an IBM TS3310 with four expansions. It has a capacity to hold up to 346 tapes available for processing by 11 IBM LTO-5 Tape Drives. LTO-5 refers to a type of tape media that follows the fifth generation of the Linear Tape Open standard, a commonly used standard magnetic tape format that has a capacity to hold 1.5TB (terabytes) of uncompressed data. The IBM TS3310 is a type of tape library system that is also referred to as an ATL, or automated tape library system. It utilizes modern robotic arm technology that largely eliminates the need for manual loading and unloading of tapes for processing by tape drives. All tapes are automatically encrypted to protect against accidental exposure.

D. System and Data Recovery

Users of the County's enterprise data systems can request the restoration of any of their files stored on DoIT managed file servers through the helpdesk ticketing system. Requests for recovery of files backed up within the prior 35 days are generally satisfied in 24 hours or less. File versions older than 35 days take longer since those backups have been migrated to tape and sent to off-site storage, and thus need to be returned to the data center before recovery can be accomplished. Database data records may also be similarly recovered upon request.

Beyond this database record and file level recovery process, DoIT also must plan for larger scale system level recoveries. This level of recovery usually derives from the occurrence of some major event, such as a power outage or complete system corruption or failure. As reported to the Grand Jury during interviews, the most recent examples of this category are the power outages caused by the PG&E Public Safety Power Shutoff (PSPS) program. DoIT has developed, and continues to maintain and improve, its power shutdown and power up procedures for their data centers. The PG&E PSPS incidents this last fall provided DoIT with the opportunity to test these procedures. DoIT reported that no significant discrepancies in their procedures were discovered.

One area that is lacking, according to DoIT, is the development of a comprehensive business continuity plan. This type of plan would outline processes, procedures and resources to use in case of a major disaster occurring in the vicinity of the data centers causing them to be inaccessible. A business continuity plan would include components outside DoIT and require coordination with other County business units and departments. It would also require the implementation of a testing plan, preferably at least annual, to ensure that all critical personnel understand their role and how to perform their duties in accordance with the plan.

V. FINDINGS AND RECOMMENDATIONS

FINDING 1 – Enterprise System Catalog - The County created an enterprise system catalog by the due date of July 1, 2016 in compliance with Government Code section 6270.5. It was

completed and posted on the County's website in a location accessible to the public. However, the subsequent annually updated files had not been posted to the website.

RECOMMENDATION 1 – Annual review procedures need to be amended with the requirement to post the updated enterprise system catalog to the County's website.

FINDING 2 – County Assessment and Taxation System Project – This is the replacement project for the Solano County Integrated Property System. The project has a $10 million reserve set aside and presents significant risk and expense to the County.

RECOMMENDATION 2 – DoIT Project Manager monitor the Project Plan deliverables, timelines, and activities relating to budget status and any changes in anticipated staffing needs. Provide regular status reports to the Board of Supervisors and stakeholder departments.

FINDING 3 – System and Data Recovery – At the time of this report, the comprehensive disaster recovery and business continuity plan outlining processes, procedures and resources was incomplete. DoIT management disclosed improvement was needed in this area and they were addressing at the onset of the review.

RECOMMENDATION 3 – The CIO and senior staff continue to thoroughly review and update plans to ensure they are up-to-date and routinely tested. Documentation should completely outline processes, procedures and resources to be used in case of a major disaster occurring in the vicinity of the data centers causing them to be inaccessible. This will be an essential tool in the effective operation of Solano County government in case of a major regional disaster event.

REQUIRED RESPONSES (ALL FINDINGS)

Solano County Department of Information Technology Chief Information Officer

COURTESY COPIES

Solano County Administrative Officer
Solano County Board of Supervisors
Solano County Auditor-Controller
Solano County Assessor/Recorder
Solano County Treasurer-Tax Collector-County Clerk