



INFORMATION TECHNOLOGY

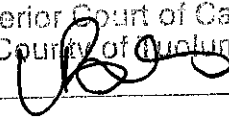
gpc

County of Tuolumne
www.tuolumnecounty.ca.gov
2 South Green Street
Sonora, CA 95370
Phone (209) 536-2360
Fax (209) 536-2361

August 4, 2017

FILED

AUG 10 2017

Superior Court of California
County of Tuolumne
By:  Clerk

Judge of Superior Court
Honorable Kate Powell Segerstrom
Tuolumne County Superior Court
60 North Washington Street
Sonora, CA 95370

Re: Response to Grand Jury Report – Information Technology Department

Dear Judge Powell-Segerstrom:

The following is offered in response to the 2016-2017 Grand Jury Report as it pertains to the Information Technology Department

Grand Jury Findings – Information Technology

F1. IT staffing was significantly reduced starting in 2008, but expectations have grown, leading to the inability of the IT Department to deliver what county departments are asking for in a timely manner.

Response: Agree. The latest IT reorganization has helped remedy this finding.

F2. There is no IT director. The IT manager reports to a deputy CAO causing a possible conflict of interest. The CAO is responsible for budgeting, and this can conflict with the interests of the IT Department leaving no one at the Director level to advocate on behalf of the IT Department.

Response: Agree.

F3. The IT Project demands from multiple departments throughout the county creates delays in many projects and conflicts between departments.

Response: Agree. The latest IT reorganization has helped remedy this finding.

F4. Security falls under Risk Management, which is the responsibility of Human Resources. The IT Department operates in a manner where security is not its

responsibility, creating serious security and reliability issues throughout the county.

Response: Agree. The Information Security Officer (ISO) does reside in risk management.

Response: Disagree. IT personnel are all very interested in maintaining a secure IT environment.

F5. IT Department staff are constantly “putting out fires” and do not have a lot of time to train. Training is often interrupted in order to work on issues.

Response: Agree.

F6. County facilities do not take into account the needs of IT equipment, leading to critical county infrastructure being in danger of destruction if fire suppression equipment were activated.

Response: Agree. Fire suppression in computer environments is a hotly debated topic as there is not a good affordable solution to fire suppression in computer rooms.

F7. Labor and cost estimates for projects have consistently been underestimated and have suffered from scope creep contributing to delays in project delivery.

Response: Agree.

F8. The projects of highly “visible” departments are prioritized while other work is deprioritized, impacting long-term projects and Maintenance and Operations.

Response: Agree.

F9. The Tuolumne County IT Department has no consistent project tracking system, does not break work into milestones, and cannot provide immediate project status reports.

Response: Agree. The IT department found that there was significant overhead to managing projects with Microsoft Project and have stopped using the product.

Response: Disagree. Projects are overseen by IT analysts who report and manage project progress.

F10. There is no formal policy for documentation of processes, procedures, or work performed. Documentation is not mandated, nor is it consistent. Documentation should be written to both account for how software or equipment is installed or maintained, and also to permit others to learn how

the work was done. Accurate and complete documentation eases the burden for future maintenance, and allows the work to be reproduced if additional equipment or software must be configured in the same way.

Response: Agree. While all software installs are documented and maintained, there is no formal policy that defines that activity.

F11. Staff are not given sufficient time to perform infrastructure maintenance.

Response: Agree.

F12. There is no security analyst or specialist in the IT Department. Lack of sufficient time for existing staff to address security issues proactively, and no dedicated security staff, leaves the county at increasing and unnecessary security risk.

Response: Agree. Although there is not a security analyst in the IT department every member of the team makes security a priority.

F13. There is no formal Password Protection Policy (PPP). No complexity requirements are required for some systems and no password expirations are imposed. No requirements or limitations exist for password reuse, sharing, distribution, storage, or breach reporting. Lack of clear password rules reduces overall security, allowing for common and reused passwords to ease the effort involved in hacking any account from years or months to as little as seconds.

Response: Agree.

F14. There is no current formal Disaster Recovery Plan/Policy (DRPP). Without a formal plan to address disaster response, any reaction will have to be created under duress, without the time or forethought that proper planning provides.

Response: Agree.

F15. There is no current formal backup retention/Data Retention (DR) policy. Data backups are kept at most for one year and for as little as two weeks. This may conflict with transparency and data retention requirements under the California Public Records Act and California Government Code §26202.

Response: Agree. Backups are scheduled and maintained but there is not a formal policy on the management of the backups.

F16. There are no persistent email archives. While some emails will not be required to be kept, some email messages are parts of the decision-making process, and records may be required. This may conflict with transparency and data

retention requirements under the California Public Records Act and California Government Code §26202.

Response: Agree.

F17. There is no formal training policy. Continuing education is critical for any organization, but particularly one where a failure to address issues in a timely fashion will incur costs that must be shouldered by county taxpayers.

Response: Agree.

F18. There is no formal policy for Secure Data Destruction (SDD) and/or drive wipe before decommissioning old hardware. Failure to consistently destroy sensitive information leads to significant security and privacy risks.

Response: Agree. There is no formal policy for SDD.

Response: Disagree. There is a procedure that is followed that meets DOD standards.

F19. There is no formal Information Logging Standard (ILS) policy, or Security Information and Event Management (SIEM) policy or procedure for log, hardware, software, or reporting audits which prevents compliance with HIPAA and PCI DSS, prevents accurate source-tracking for infections, and places the weight of IT on emergency response instead of planned and coordinated activities.

Response: Agree. There is no formal policy for ILS.

Response: Disagree. While log monitoring and reporting are taking place there is not a formal policy in place to define this activity.

F20. There is no formal policy for ongoing SB272 (§6270.5 of the California Public Records Act) compliance, which may violate SB272.

Response: Agree. There is not a formal policy for SB272 compliance.

Response: Disagree. Tuolumne County has published and updated the system catalog required by SB272.

F21. There are no formal policies or procedures in place for maintaining IT equipment in Tuolumne County leading to grossly out of date networking equipment, security equipment, and other systems being years behind in required maintenance.

Response: Agree.

F22. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires regular software and Operating System (OS) maintenance, as well as regular review and auditing to remain in compliance with steep penalties for failure.

Response: Agree.

F23. The Payment Card Industry Data Security Standard (PCI DSS) requires any organization collecting payments via credit card to perform regular security maintenance, complete application maintenance, restrict physical access to devices that can access cardholder data, regularly test device and network security, create and maintain an Information Security (InfoSec) policy, store logs for a minimum of one year, and perform log audits.

Response: Disagree. Tuolumne County uses outside vendor systems for collecting payments via a credit card.

F24. The county does not have a Reverse Whois (RWhois) record, which provides third parties a direct contact for issues relating to any network issues discovered such as botnet, malware, or spam originating from their network.

Response: Agree.

F25. The county has hundreds of IP addresses assigned, though only 21 named devices, many of which do not require a dedicated IP address. The allocation of this many IP addresses to an organization that is not using them efficiently violates the Number Resource Policy Manual (NRPM), which requires a minimum 50% utilization of allocated IPv4 resources. IPv4 exhaustion is here and more than 200 IP addresses are being wasted by Tuolumne County.

Response: Disagree.

F26. The Morning Star facility lacks security cameras.

Response: Agree.

F27. The Morning Star facility lacks physical security for the server room.

Response: Agree.

Response: Disagree. The Morningstar network closet does have physical locks that limit access.

F28. The Morning Star facility server rooms use sprinklers for fire suppression.

Response: Agree.

F29. The Morning Star facility server room leaves tape backups exposed.

Response: Agree. The Morningstar facility network closet has sprinklers.

Response: Disagree. The Morningstar facility network closet is protected with locked doors with limited access.

F30. The NOC leaves tape backups exposed.

Response: Agree.

F31. The NOC uses sprinklers for fire suppression.

Response: Agree.

F32. There is no formal policy for supervised third-party NOC access, which violates HIPAA, PCI DSS, and creates other potential security issues.

Response: Agree. IT staff has been directed to supervise outside visitors but there is not a formal policy.

F33. The current ticketing platform is outdated and unsupported. It does not enforce tracking of important data, creating inconsistent records. This prevents preemptive action to address hardware, software, and end-user issues.

Response: Agree.

F34. The existing SAN is full, making long-term backups and recovery impossible, and creating a situation where staff need to prioritize what electronic records departments can retain. Certain records must be kept for two years under California Government Code §26202, and it appears that this is not being done.

Response: Agree.

F35. Firmware updates that address security vulnerabilities are being neglected for every single network access device - router, switch, wireless access point, firewall, and enterprise appliance - in the fleet.

Response: Agree. A large portion of our network devices do not have the latest firmware. There is not a formal policy for maintaining hardware firmware levels.

Response: Disagree. Critical devices on the edge of the network do get firmware updates as deemed necessary.

F36. IT Department staff are not monitoring vendor websites for patch information, allowing hardware and software to remain insecure and years out of date, making county devices easy targets for attackers.

Response: Disagree. All IT staff members monitor different websites and blogs.

F37. IT Department staff are not consistently participating in mailing lists, newsgroups, guides, forums and other patch management systems, limiting their exposure to information about updates, processes, and issues to address known problems.

Response: Disagree. All IT staff members participate in different mailing lists, newsgroups, guides and forums.

F38. Servers throughout the county are out of date and some critical services run on software that is eight years beyond EOL, placing them at severe security risk and increased risk of instability.

Response: Agree.

Response: Disagree.

F39. IT does not patch servers with the majority of applicable updates, leaving them insecure.

Response: Agree.

F40. The current update process does not consistently include Canary Testing, placing all devices at increased risk of collateral failure.

Response: Disagree. IT uses a staged approach when rolling out enterprise wide patches and updates.

F41. Nearly all of the updates that are installed are delayed a month, then installed on all affected devices simultaneously during normal business hours. This interrupts normal business processes and increases the risk associated with these devices until they are patched.

Response: Disagree. Updates are not delayed a month. IT uses different strategies for different levels of patches and updates.

F42. Line of business applications (as many as 300 separate applications) are not consistently maintained, leaving critical applications potentially unstable and insecure.

Response: Disagree.

F43. Post-update device restarts are not being forced, allowing devices to remain insecure until the user chooses to restart manually.

Response: Disagree.

F44. Most user devices are still running 32-bit Operating Systems (OS) because a 64-bit OS image has not yet been approved for county-wide use, wasting resources within each device and slowing device performance, impacting Tuolumne County staff time.

Response: Agree.

F45. Some critical line of business applications can no longer be used or upgraded because they require 64-bit Operating Systems (OS), leaving departments unable to function.

Response: Disagree. Users and applications that require 64bit operating systems are accommodated with special version images.

F46. Not all staff are fully trained in their Remote Monitoring & Management (RMM) solutions, requiring manual intervention for diagnostics and reporting, wasting time and resources.

Response: Agree. Each IT unit requires different levels of RMM access.

F47. Malware infections are a daily occurrence and only those reported to IT are discovered and addressed. The resolution for most infections on Tuolumne County hardware is to reimage the device (or devices), which causes loss of user data and prevents data collection for sourcing infections to determine intent (such as spear phishing, ransom, botnet, or general infection), which prevents adequate response to targeted attacks.

Response: Agree. Re-imaging devices is the best way to make sure you have eradicated a malware infection. Users should not lose data as they have been directed to not store data on the local machine.

Response: Disagree. Malware infections are NOT a daily occurrence.

F48. Ransomware has taken down parts of the network on multiple occasions, also causing server data breaches. Servers have no defense enabled against network-aware malware or user negligence.

Response: Agree. Tuolumne County has been hit by a couple of Ransom Ware attacks with very limited impact.

Response: Disagree. Tuolumne County has been hit by a couple of Ransom Ware attacks with very limited impact. Due to the security measures in place we have been able to isolate and remedy Ransom Ware attacks with very little loss of data.

F49. Tuolumne County is using software firewalls that are EOL, putting the entire county infrastructure at risk.

Response: Agree. Tuolumne County uses one (1) software firewall.

F50. Tuolumne County is using hardware firewalls that are EOL, putting the entire county infrastructure at risk.

Response: Agree.

F51. Physical access to devices is possible in every department the Grand Jury visited. Toolkits that allow network-level hijacks are available online for under \$50, so one doesn't need to be a "highly-financed state-sponsored actor" to be able to hijack Tuolumne County networks.

Response: Disagree. Physical access is limited through Security Policy and proper security practices.

F52. Physical access to network ports is possible in almost every department the Grand Jury visited, exposing the network to security risks.

Response: Disagree. Physical Access to network ports is controlled and limited through a Network Access Control (NAC) device.

F53. There is no Network Device Integrity (NDI) Methodology in place which creates inconsistency in security response to network issues.

Response: Agree.

F54. Sender Policy Framework (SPF) is not in use, exposing Tuolumne County to potential abuse from spam messages and phishing messages with forged address from Tuolumne County addresses.

Response: Agree.

F55. Domain Keys Identified Mail (DKIM) is not in use, exposing Tuolumne County to potential abuse from spam messages and phishing messages with forged address from Tuolumne County addresses.

Response: Agree.

F56. No formal policy or process is in place for external vendor access, creating inconsistency and potential security issues.

Response: Agree. While best practices are used there is not a formal policy regarding vendor access.

F57. Several website security issues exist.

Response: Disagree. Not defined.

F58. Websites use expired or no SSL certificates, increasing the risk of data leakage or compromise.

Response: Disagree. All sites requiring certificates are protected.

F59. The Bring-Your-Own-Device (BYOD) management platform is externally visible, exposing the entire network to abuse.

Response: Agree.

F60. The county website does not support SSL.

Response: Disagree. The County website DOES support SSL.

F61. There are several domains that present the same content for the Tuolumne County Website, impacting Search Engine Optimization (SEO) efforts and canonicalization.

Response: Disagree.

F62. The robots.txt file Sitemap reference is invalid.

Response: Agree.

Grand Jury Recommendations – Information Technology

R1. Hire at least two mid-level industry-experienced IT professionals to increase the capacity of the department. (F1)

Response: IT has made a request to the CAO office for a priority restoration of two (2) analyst positions.

R2. Hire one more technical support analyst to assist county users who require help. (F1)

Response: IT has made a request to the CAO office for a priority restoration of one (1) technician position.

R3. Hire a Chief Information Officer (CIO) or IT Director that would report directly to the CAO and not a deputy CAO. That individual must have an experienced IT background and not have any other responsibilities within the county administration. Should the position not be created/filled, we request that the CAO, BOS and County Counsel explain why the current arrangement is not a conflict of interest. (F2)

Response: IT would support the hiring of a CIO or IT Director.

R4. All County departments must be made aware of needs of the other departments and work together to prioritize their IT needs. (F3)

Response: IT will make extra efforts during the Information Technology Steering Board process to fully explain the needs of all departments.

R5. Security training must take place for members of the IT Department. It is preferred that training take place offsite instead of online or on-site training, so they are not interrupted during training. (F4, F5)

Response: IT supervisors will be tasked with a goal on their performance evaluations to develop a training plan for each member of their group. With each training plan the supervisors will be required to tie back the training plan to security initiatives.

R6. Involve the IT Department in all aspects of planning and implementation of how buildings are set up for proper IT infrastructure. The IT Department should be included in final approval of County building plans. (F6)

Response: With the development of the Law & Justice Center it has become apparent that all construction activities should involve a plan to support Information Technology services. The IT department has worked closely with the CAO office to communicate the need for IT involvement in all construction efforts.

Response: With the new assignments in the CAO office both Facilities and Information Technology report to the same manager. This will improve communications during construction efforts.

R7. Investigate project management methodologies such as Agile, Lean, and Kanban. The Jury also recommends that the county investigate software for project management to improve project estimation and tracking capabilities. (F3, F7, F9)

Response: IT will explore options available for Project Management software.

R8. Prioritize projects based on the needs of the entire county, both government and citizens. All projects and project requests should go through the standard ITSB procedures, and prioritization should also include maintenance on IT equipment so that technical debt is not accrued. (F8)

Response: IT will revamp the ITSB procedures to ensure proper attention is paid to maintenance of IT infrastructure.

R9. Create an up-to-date and actively maintained knowledge base about how networks, hardware, and software are installed and configured. (F10)

Response: IT will formalize a policy and create a procedure for maintaining and updating an IT knowledge base (document library) of; network configurations, hardware configuration and setup, and detailed software installation documentation.

R10. Modify IT Department work schedules to stagger some staff so some Maintenance & Operations can be performed after hours in other departments. (F11)

Response: IT will work with the CAO office and department heads to create a regular maintenance window for Maintenance & Operations. IT supervisors will work with team members to create workable schedules to support the newly created maintenance window.

R11. The Grand Jury strongly recommends hiring a dedicated security analyst. (F4, F12)

Response: The IT department takes security very seriously and would support adding a dedicated security analyst.

R12. Create, maintain and observe a Password Protection Policy (PPP) that incorporates complexity requirements, password expiration, limits reuse, sharing, distribution, and storage, and requires breach reporting. (F13)

Response: The IT department will work with the CAO Office, County Counsel and department heads to develop a PPP that incorporates; complexity requirements, password expiration, limits reuse, sharing, distribution, and storage, and requires breach reporting.

R13. Create, maintain and observe a Disaster Recovery Plan/Policy. (F14)

Response: The IT department will update the current Disaster Recovery Plan.

R14. Create, maintain and observe a Data Retention (DR) policy for email, data, and stateful work that complies with California law and the Freedom of Information Act (FOIA). (F15, F16)

Response: The IT department will work with County Counsel to develop and document a formal data retention policy that address's data storage and E-Mail. The IT department will develop procedures and documentation to support the developed data retention policy

R15. Create, maintain and observe a formal IT Training Policy that incorporates best practices for documentation, maintenance, security, monitoring, and ensures that attendees are not pulled away during training. (F17)

Response: IT will develop a formal department training plan that ensures employees receive adequate security training.

R16. Create, maintain and observe a Secure Data Destruction (SDD) policy. (F18)

Response: IT will create a formal policy for Secure Data Destruction. The policy will utilize the current SDD process that fully meets Department of Defense (DOD) requirements.

R17. Create, maintain and observe an Informational Logging Standard (ILS) policy and Security Information and Event Management (SIEM) policy and procedure, ensuring that logs are regularly and actively audited. (F19, F22,F23)

Response: IT will create a formal policy for Security Information and Event Management (SIEM). The policy will document and refine the current IT process.

R18. Create, maintain and observe a policy for ongoing SB272 (§6270.5 of the California Public Records Act) compliance. (F20)

Response: An IT policy will be created and maintained to meet SB272 compliance.

R19. Create, maintain and observe a policy and procedure for maintaining network equipment (routers, switches, firewalls, wireless access points, peripherals, and enterprise appliances) that incorporates no less than weekly firmware checks and vendor monitoring for all network equipment, and decommission planning for hardware approaching EOL. (F21, F35, F36, F37)

Response: IT will create, maintain and follow a policy to maintain a reasonable maintenance schedule for network equipment. IT will create, maintain and follow procedures to maintain a reasonable maintenance schedule for network equipment. IT

will create, maintain and follow procedures to maintain a reasonable hardware life cycle for network equipment.

R20. Create, maintain and observe a policy and procedure for maintaining end-user equipment that incorporates Canary Testing, Operating System(OS) updates and monitoring, application updates and monitoring for all installed applications, update installation windows outside of individual department business hours, force system restarts outside of individual department business hours, change monitoring to identify irregular activity, and replacement planning for hardware, applications, and Operating Systems approaching EOL. (F21, F36, F37, F40, F41, F42, F43)

Response: The IT Department is currently working on a policy and procedure to update, maintain and monitor end-user equipment.

R21. Create, maintain and observe a policy and procedure for maintaining server equipment that incorporates Canary Testing, Operating System (OS) updates and monitoring, application updates and monitoring for all installed applications and services, change monitoring to identify irregular activity, and replacement planning for hardware, applications, and Operating Systems approaching EOL. (F21, F36, F37, F38, F39, F40, F42, F43)

Response: IT will create, maintain and follow a policy to maintain a reasonable maintenance schedule for server equipment. IT will create, maintain and follow procedures to maintain a reasonable maintenance schedule for server equipment. IT will create, maintain and follow procedures to maintain a reasonable hardware life cycle for server equipment.

R22. Create, maintain and observe a policy and procedure for HIPAA compliance. Each affected Department should be aware of their obligations and actively participate and pursue full compliance. (F22)

Response: IT will create a policy and procedure for HIPAA compliance from an IT support perspective. IT will support Policies' and Procedures that are developed by individual departments.

R23. Create, maintain and observe a policy and procedure for PCI DSS compliance. Each affected Department should be aware of their obligations and actively participate and pursue full compliance. (F23)

Response: The IT department will create a policy for the handling of PCI processes.

R24. Direct the county's Internet Service Provider to create an RWhois record and populate it with appropriate role-based contact information. (F24)

R31. Replace the sprinklers with HFC-227ea fire suppression systems, or any other electronics-friendly fire suppression system, within the NOC. (F6, F31)

Response: The IT department will work with Facilities to identify workable solutions to fire suppression at the Network Operation Center.

R32. All third-party access to the NOC should be supervised and logged. (F32, F56)

Response: A policy will be created to control and document all third party access to the NOC.

R33. A replacement ticketing platform must be researched, obtained, and implemented as soon as possible. The replacement ticketing platform should enforce device, user, and technician identification, and provide for canned responses, Frequently Asked Questions (FAQ), Knowledge Base (KB), and self-help integration for ticket submission, multiple support queues and automated technician/group assignment. The county must create, maintain and observe a policy and procedure for ticket, FAQ, and KB management, and require ticket data audits on a weekly basis. (F33)

Response: IT will define requirements and research available product offerings for a comprehensive Information Technology management system. The IT department will add a request for an Information Technology Management system in the mid-year budget request.

R34. The SAN upgrade must be completed with the highest priority. The SAN must be installed within 30 days of publication of this report. (F34)

Response: The IT department has engaged a service provider to expedite the full implementation of the SAN. Work will be completed by August 2017.

R35. Complete and actively maintain a hardware audit to obtain an accurate Asset Management accounting of actual network devices in use throughout all county facilities. The audit should include the exact location, make, model, serial number, patch level with firmware hash, installation date, observation date, MAC address, routable addresses, department affiliations, responsible parties and any other applicable notes. Vendor websites should be actively monitored for each device model for updates and EOL. This Asset Management system should be integrated into the Network Analyst's workflow to ensure that all hardware is properly observed and maintained. (F35, F36, F37)

Response: While the IT department currently maintains a library of all installed hardware the data is not as extensive as requested here. IT will add extended data requirements to the Asset Management module of the Information Technology management system.

R36. County IT staff should be mandated to participate in online forums and mailing lists related to their duties. This should include SANS, SANS Internet Storm Center (ISC), the National Institute of Science and Technology (NIST), NIST's Computer Security Resource Center (CSRC), the Internet Engineering Task Force (IETF), US Computer Emergency Readiness Team (US-CERT), CSO , Patch Management , SaferPC , and the various Stack Exchange sites. (F36, F37)

Response: The IT department does participate in online forums, mailing lists and other technology related information sites.

R37. Wherever possible, EOL devices should be replaced or terminated. Where this is not possible, we recommend that alternatives, such as Microsoft Premium Assurance, be sought out to minimize collateral damage from unsecurable devices. (F38)

Response: IT will investigate the use of Microsoft Premium Assurance where necessary.

R38. Immediately prepare and approve a 64-bit Operating System image and gradually roll it out to all supported devices, prioritizing those departments that require 64-bit Operating Systems for line of business applications. Approval should occur within 90 days of publication of this report. (F44, F45)

Response: The IT department has been working on Windows 10 deployment for several months with a scheduled roll-out beginning in August 2017.

R39. All IT staff need to be actively trained in the RMM solutions. (F46)

Response: All applicable IT staff have/will be trained in the various RMM solutions used in Tuolumne County.

R40. Create, maintain, and observe a policy and procedure for malware events that does not treat them as a mere nuisance, but treats each incident as a potential disaster. Each affected device should be fully audited and user logs should be actively reviewed until the source of the observed infection and any other identified infections can be rooted out. Detection signatures and edge rules should be modified to address any discoveries, thus preventing similar

infections in the future. Any infected users should be required to attend end user security training. (F47)

Response: The IT department is comfortable with our current Malware procedure. IT will work to create a policy that documents and supports our current process. The IT department will identify and deploy training courses to educate users on identifying and reacting to Malware events.

R41. Immediately install and maintain File Server Resource Manager (FSRM) on all servers for ransomware signatures. User accounts triggering events matching ransomware signatures should be immediately locked out across the network, with alerts being sent to Network Analysts and Technicians for fast response. Likewise, bulk erases, often a result of user error, should lock out accounts and trigger Network Analysts response. This should be performed within 10 days of publication of this report. (F48)

Response: The IT is currently deploying security devices that will identify potential security issues. IT will pursue the use of File Server Resource manager for use in our environment.

R42. Immediately replace all hardware and software firewalls. (F49, F50)

Response: Hardware firewalls completed, July 2017. Software firewall replacement scheduled, August 2017.

R43. Perform regular on-site inspections of all county facilities to inspect the state of all hardware, validate that devices have not been physically compromised or tampered with, move physically susceptible devices away from locations where guests have access, and look for susceptible network access points. Susceptible access points should trigger a work order for facilities management to remove the accessible port. Technicians should document and photograph all hardware and network access points on each visit for their records. (F51, F52)

Response: County IT currently employs security controls that prohibit these types of attacks.

R44. Create, maintain, and observe a policy and procedure for Network Device Integrity (NDI) Methodology. (F53)

Response: IT will create a policy and procedure for Network Device Integrity (NDI).

R45. Implement an SPF record for all county domains, even those domains that are not actively in use. This simple DNS text record for SPF compliance is likely

as easy as running this command on their DNS servers: dnscmd /recordadd co.tuolumne.ca.us TXT "v=spf1 ip4:50.203.5.128/29 a mx -all" Repeat for all domain names. This should be performed within 10 days of publication of this report. (F54)

Response: IT will implement SPF records where required.

R46. Implement DKIM for all county domains and mail relaying servers. (F55)

Response: IT will implement DKIM where required.

R47. Create, maintain, and observe a policy and procedure for external vendor access that integrates the Principle of Least Privilege (POLP), mandates audits of vendor activity, and requires logging of all vendor access within the ticketing platform. (F56)

Response: IT will create a policy and procedure for vendor access, modeled after our current process.

R48. Immediately patch websites and actively monitor vendor websites for updates. (F36, F37, F57)

Response: The IT network team is working to update/patch all of our current internet services.

R49. Disable and remove all websites that are no longer in use. (F36, F37, F57)

Response: IT will disable and remove all non-active websites.

R50. Enable and maintain SSL on all county websites. Renew expired certificates. (F58, F60)

Response: Where appropriate all secure websites have updated certificates. Not all websites require security certificates.

R51. Disable external access to the BYOD website. If that is not possible due to remote activation constraints, enable and require port-knocking to ensure that unauthorized users cannot abuse the site. (F59)

Response: IT will investigate this recommendation and employ proper security on our MDM platform.

R52. Select one preferred domain name and perform an HTTP 301 Redirect from all other variations to the preferred domain. (F61)

Response: IT believes that we are using our domain names appropriately.

R53. Correct the robots.txt file to conform with the Sitemaps standard. (F62)

Response: IT will correct any deficiencies with our robots.txt file and repair any anomalies.

Sincerely,



ROBERT CHAPMAN
Information Technology Manager

Sincerely,



DANIEL RICHARDSON
Deputy County Administrator

cc: Sherri Brennan, Chair, Board of Supervisor
Craig Pedro, County Administrator