STATE OF ARIZONA

Department of Revenue

Douglas A. Ducey
Governor

David Raber
Director

September 25, 2015

Debra K. Davenport, CPA
Auditor General
Office of the Auditor General
2910 North 44th Street, Suite 410
Phoenix, AZ 85018

RE: Arizona Department of Revenue Sunset Review; Revised Draft Report “Arizona Department of Revenue – Security of Taxpayer Information” dated September 18, 2015

Dear Ms. Davenport:

Thank you for the opportunity to review the revised performance audit report focusing on the security of taxpayer information at the Arizona Department of Revenue (ADOR).

Securing our citizens’ personal data is of the utmost importance to ADOR. We have made great strides in continuously improving our data security operations. We appreciate the insight provided by your audit team, and will implement your recommendations in an effort to further improve our processes.

Attached are the ADOR responses to your audit findings.

We look forward to sharing our progress as we continue to address the recommendations offered in your report.

Sincerely,

David Raber, Director

Attachment

Response from Arizona Department of Revenue (ADOR) to the Auditor General's report on Security of Taxpayer Information

FINDING 1

1.1 In conjunction with completing the implementation of its information security program (as recommended in Finding 2), the ADOR should develop and implement written procedures for structured vulnerability assessments of its IT infrastructure. These procedures should include requirements to:

a. Ensure all systems are included in vulnerability scanning, such as using automated tools to discover systems on the network;

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: ADOR is currently modifying its vulnerability scanning procedures and software configurations to employ host discovery methods (ping) to determine which hosts are to be scanned on every subnet. Furthermore, ADOR will be deploying a rogue system detection capability to ensure that no systems escape the weekly vulnerability scan.

b. Regularly conduct vulnerability assessments that determine whether security requirements and controls are functioning effectively;

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: ADOR conducts annual vulnerability assessments of its systems, networks, and applications. Due to the ever changing cyber threat environment ADOR will implement governance to direct dynamic and agile assessments in support of continuous monitoring and the risk assessment process. Procedures will be updated to reflect current practices and remediate the finding.

c. Analyze vulnerabilities to determine their impact on systems and the associated risk;

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: ADOR will implement a robust vulnerability assessment process aligned with industry best practices and National Institute of Standards and Technology (NIST) guidance which will include methods of determining the impact and residual risk to ADOR systems. Procedures will be updated to reflect current practices and remediate the finding.

d. Review and then remediate, based on risk, the problems identified during these vulnerability assessments;

   RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

   STATUS: Improvements to ADOR risk identification and management processes are currently under way. Enhancements and efficiencies via a tool that can streamline and automate remediation efforts are being evaluated for incorporation. Procedures will be updated to reflect current practices and remediate the finding.

e. Accept the risk of weaknesses that cannot be mitigated;

   RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

   STATUS: ADOR is currently evaluating the Change Management system processes to include this capability in the next generation of our service management tool. Procedures will be updated to reflect current practices and remediate the finding.

f. Assign roles and responsibilities to each task to ensure the process is performed in a timely manner;

   RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

   STATUS: ADOR policies, roles and responsibilities are currently in the process of being updated. These updates will include the changes necessary to remediate the finding.

Additional Feedback re: Current processes in place and/or action taken for Finding 1.1:

Vulnerabilities are addressed through ADOR's request management system. Tickets are open, assigned and tracked to address vulnerabilities. Escalation, incident management reporting, including but not limited to the Daily report, and Daily Operations meetings review progress on high risk problems. Automated tools exist to discover systems on the network. Vulnerability assessments occur annually.

1.2 The ADOR should document and enhance its existing process for updating and maintaining IT software and systems. Specifically, it should develop and implement written policies and procedures and ensure that these policies and procedures are followed. These written policies and procedures should address the following processes:

a. Determining and documenting whether or not a software or system update should be applied;

   RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

   STATUS: ADOR is currently evaluating its change/lifecycle management policies and procedures to incorporate industry best practices that enable and compliment the current patching policy, procedures, and system.

b. Addressing identified vulnerabilities, or accepting, justifying, and documenting the risk of not updating the software or system if there are extenuating circumstances;

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: ADOR is currently evaluating the full implementation of the NIST Risk Management Framework (RMF) that will incorporate the recommended changes.

c. Testing and documenting the effectiveness and potential side effects of available updates before installation;

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: Core system patches are applied in Test environments, then to Quality Assurance and successively to Production after assuring the patch has no negative impact to agency operations. However, ADOR is evaluating its current patch management process to identify efficiencies and incorporate industry best practices. Policies and procedures will be updated to reflect current practices and remediate the finding.

d. Ensuring that patches are installed in a timely manner;

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: ADOR currently has processes in place to apply Operating System patches within 30-days of release, however ADOR is evaluating its current patch management process to identify efficiencies and incorporate industry best practices to adapt methodologies to support 3rd party application patches. Furthermore, ADOR is evaluating a tool to automate our 3rd party application remediation processes that would reduce the timeline for patch deployment. Policies and procedures will be updated to reflect current practices and remediate the finding.

e. Reviewing updates to ensure all are applied successfully;

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: The ADOR Change Management Process, in support of Change Management Policy, already requires testing, validation and results that determine whether updates, including patching, were successful. However, ADOR is evaluating its current patch management process as a part of continuous improvement. Policies and procedures will be updated to reflect current practices and remediate the finding.

1.3 The ADOR should develop and implement written policies and procedures for securely configuring IT systems. These policies and procedures should include:

a. Requirements for configuring the IT systems so that they do not provide more functionality than is necessary, including provisions and controls to ensure that unauthorized or unneeded software is not installed or used;

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: ADOR policies, roles and responsibilities are currently in the process of being updated. These updates will include the changes necessary to remediate the finding.

b. Developing and documenting baseline configurations for each IT system, as appropriate;

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: ADOR is currently updating its system configuration documentation to develop a baseline configuration for desktops, servers, databases, network infrastructure, etc. as part of its requirements under the Change Management process. Furthermore, ADOR policies, roles and responsibilities are currently in the process of being updated. These updates will include the changes necessary to remediate the finding.

c. Developing and documenting specific configuration settings;

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: ADOR is currently updating its system configuration documentation for desktops, servers, databases, network infrastructure, etc. as part of its requirements under the Change Management process. Furthermore, ADOR policies, roles and responsibilities are currently in the process of being updated. These updates will include the changes necessary to remediate the finding.

d. Ensuring default credentials are changed;

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: ADOR is currently revamping its development procedures to include security assessments that will look for these types of items before they are put into production.

e. Defining the frequency of reviews and updates to the configurations;

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: ADOR continues to comply with Change Management Policy and Process to ensure review of changes to configurations in the required timelines. ADOR will continue to evaluate and update its policies and procedures as part of continuous improvement.

1.4. The ADOR should improve management of access controls across IT systems. These improvements should include developing and implementing written policies and procedures for:

a. Reviewing file share rights, as appropriate, to ensure unnecessary access is not granted to users;

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: ADOR policies, roles and responsibilities regarding the periodic review of user rights by management are currently in the process of being updated. These updates will include the changes necessary to remediate the finding.

b. Reviewing and adjusting, as needed, user access and account access privileges periodically;

   RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

   STATUS: ADOR policies, roles and responsibilities regarding the periodic review of user rights by management are currently in the process of being updated to remediate the finding. These updates will include mandating periodic audits of user access rights by the ISO and ADOR security team.

c. Ensuring appropriate separation between highly privileged accounts and standard user accounts;

   RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

   STATUS: ADOR will evaluate its policies and procedures to ensure separation of roles within its systems are correctly defined. ADOR will also conduct an assessment of deployed systems to determine if they are configured in accordance with policy and make the necessary changes to any systems that are not in compliance.

d. Ensuring all passwords are changed on a regular basis, including establishing requirements and time frames for changing service account passwords;

   RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented

   STATUS: ADOR does in fact set general user and privileged user accounts to automatically expire per ADOR policy. ADOR will evaluate its policies and procedures to ensure that they are aligned with current best practices and regulatory guidance as part of its ongoing continuous improvement efforts. ADOR will task the ISO to conduct an assessment of each system to ensure that it is in compliance with ADOR policy.

1.5. The ADOR should develop and implement a continuous log monitoring program that includes written policies and procedures for log monitoring of critical IT activities. These policies and procedures should describe:

a. What IT systems and functions in each IT system should be logged;

   RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

   STATUS: ADOR policies, roles and responsibilities regarding the system auditing and logging are currently in the process of being updated. These updates will include the changes necessary to remediate the finding. ADOR is currently partnering with ADOA to evaluate a SIEM tool that has the capability to remediate the finding.

b. How frequently each log should be monitored;

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: ADOR policies, roles and responsibilities regarding the system auditing and logging are currently in the process of being updated. These updates will include the changes necessary to remediate the finding.

c. Who is responsible for ensuring logging occurs and reviewing logs on a regular basis;

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: ADOR policies, roles and responsibilities regarding the system auditing and logging are currently in the process of being updated. These updates will include the changes necessary to remediate the finding.

d. Standard response actions for possible detected events, including reporting the security status of the ADOR as a whole and information systems to critical personnel;

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: ADOR policies, roles and responsibilities regarding the system auditing and logging are currently in the process of being updated. These updates will include the changes necessary to remediate the finding.

e. Provisions for log security and retention;

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: ADOR policies, roles and responsibilities regarding the system auditing and logging are currently in the process of being updated. These updates will include the changes necessary to remediate the finding. ADOR has already taken steps to ensure that logs are retained as directed in retention schedules. Furthermore, ADOR is currently partnering with ADOA to evaluate a completely managed SIEM tool.

FINDING 2

2.1. The ADOR should ensure that its ISO regularly monitors ADOR-wide compliance with the information security program policies and procedures:

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: The ADOR ISO will review the facts of this finding and determine the current way-ahead. The ISO has already identified several shortfalls in oversight in the security of the development processes of systems within ADOR and is working on a Plan of Action & Milestones to address these issues. Policies and procedures will be updated to reflect current practices and remediate the finding.

2.2. The ADOR should continue to develop and implement its information security program consistent with state requirements in the areas of data classification, risk assessments, information security awareness, education and training, and incident response. Specifically, the ADOR should:

a. Develop and implement procedures for data classification that are consistent with ASET requirements, such as protecting the information based on confidentiality, and developing a data classification inventory that is updated regularly;

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: ADOR policies, roles and responsibilities regarding the implementation of the Risk Management Framework are updated annually. Future updates will include the changes necessary to remediate the finding.

b. Establish written security agreements with the external organizations that require access to its information systems that outline information system connections' security requirements;

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: The ADOR ISO is working with the Chief Disclosure Officer to address any shortfalls in the security agreements with external organizations.

c. Develop and implement ADOR-wide risk assessment procedures that are consistent with ASET requirements, including performing them annually and documenting the results and potential impacts of the identified risks;

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: ADOR policies, roles and responsibilities regarding the implementation of the Risk Management Framework are currently in the process of being updated. These updates will include the changes necessary to remediate the finding.

d. Enhance its information security awareness education and training programs and procedures so they are consistent with ASET requirements, including requiring periodic information security awareness education and training for all users and gearing it toward their job functions. This training should include more details on common attack methods, such as the identification of phishing e-mails or telephone calls and practical examples of phishing attacks to provide illustrations for employees;

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: The ADOR ISO has added this finding to the security enhancement project plan to address the identified shortfall and develop a Plan of Action & Milestones (POA&M).

e. Improve its incident response planning policy and procedures to include automated incident response processes and an information spillage response, then develop and approve an incident response plan;

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: Incident response processes are reviewed and updated annually. This review includes roles, tasks, escalation, and notification. ADOR will also review the current processes for translation into a viable continuous monitoring program that is suitable to automation.

2.3. The ADOR should develop and implement an action plan for completing the development of its information security program. This action plan should identify tasks that need to be accomplished, the resources required to accomplish these tasks, and scheduled completion dates for the milestones:

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: The ADOR ISO is currently developing a project plan to address all the identified shortfalls, integrate enhancements to the security of the department, and implement the Risk Management Framework.

FINDING 3

3.1. The Department should continue to develop and implement its new policies for annually reviewing badge access rights to sensitive areas, such as the server room:

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: ADOR is in the process of documenting its procedure in writing and expanding it as required by the finding.

3.2. The Department should maintain documentation of collecting and destroying former employees' badges. Additionally, the Department should document its badge deactivation requests to the ADOA and develop and implement procedures for monitoring badge deactivation by the ADOA and following up with the ADOA, as necessary, to ensure that badges are deactivated in a timely manner:

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: ADOR is in the process of documenting its procedure and expanding it as required by the finding.

3.3. The Department should implement additional training and supervision as needed to ensure employees comply with its clean-desk policy to prevent unauthorized access to taxpayer information:

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: ADOR will analyze and develop additional mandatory awareness training and supervision to ensure employees comply with the clean desk policy.

3.4. The Department should educate employees on the Department’s procedure for sending and receiving sensitive information on fax machines and should expand the procedure to include copy machine/printers:

RESPONSE: ADOR agrees with the finding of the Auditor General, and the audit recommendation will be implemented.

STATUS: ADOR will revise its acceptable use policy and fax machine procedure and educate employees about the revised policy and procedure.