



DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

June 24, 2016

The Honorable John Allen, Chair
Joint Legislative Audit Committee

The Honorable Judy Burges, Vice Chair
Joint Legislative Audit Committee

Dear Representative Allen and Senator Burges:

Our Office has recently completed an initial followup of the *Arizona Department of Revenue—Security of Taxpayer Information* regarding the implementation status of the 36 audit recommendations (including sub-parts of the recommendations) presented in the performance audit report released in September 2015 (Auditor General Report No. 15-116). As the attached grid indicates:

- 7 have been implemented;
- 21 are in the process of being implemented; and
- 8 have not been implemented.

Our Office will conduct an 18-month followup with the Arizona Department of Revenue on the status of those recommendations that have not yet been fully implemented.

Sincerely,

Dale Chapman, Director
Performance Audit Division

DC:ka
Attachment

cc: David Briant, Director
Arizona Department of Revenue

Arizona Department of Revenue—Security of Taxpayer Information

Auditor General Report No. 15-116 Initial Follow-Up Report

Recommendation

Status/Additional Explanation

Finding 1: Department needs to improve its IT security

<p>1.1 In conjunction with completing the implementation of its information security program (as recommended in Finding 2), the Department should develop and implement written procedures for structured vulnerability assessments of its IT infrastructure. These procedures should include requirements to:</p>	<p>The Department is developing written procedures that are in line with auditors' recommendations for conducting regular vulnerability assessments and managing identified vulnerabilities. The Department reported that it plans to implement its vulnerability-management process by August 2016 and implement regular vulnerability assessments, including third-party assessments, by January 2017.</p>
<p>a. Ensure all systems are included in vulnerability scanning, such as using automated tools to discover systems on the network;</p>	<p>Implemented at 6 months</p>
<p>b. Regularly conduct vulnerability assessments that determine whether security requirements and controls are functioning effectively;</p>	<p>Implementation in process See explanation for Recommendation 1.1.</p>
<p>c. Analyze vulnerabilities to determine their impact on systems and the associated risk;</p>	<p>Implementation in process See explanation for Recommendation 1.1.</p>
<p>d. Review and then remediate, based on risk, the problems identified during these vulnerability assessments;</p>	<p>Implementation in process See explanation for Recommendation 1.1.</p>
<p>e. Accept the risk of weaknesses that cannot be mitigated; and</p>	<p>Implementation in process See explanation for Recommendation 1.1.</p>
<p>f. Assign roles and responsibilities to each task to ensure the process is performed in a timely manner.</p>	<p>Implementation in process See explanation for Recommendation 1.1.</p>
<p>1.2 The Department 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:</p>	<p>The Department is developing and implementing written policies and procedures related to managing IT software and system updates, and some procedures have been implemented in practice. The Department is also purchasing software tools that will help identify and apply IT updates. The Department reported that it plans to implement all of the recommendations for managing IT updates by January 2017.</p>
<p>a. Determining and documenting whether or not a software or system update should be applied;</p>	<p>Implementation in process See explanation for Recommendation 1.2.</p>
<p>b. Addressing identified vulnerabilities, or accepting, justifying, and documenting the risk of not updating the software or system if there are extenuating circumstances;</p>	<p>Implementation in process See explanation for Recommendation 1.2.</p>

Recommendation	Status/Additional Explanation
<ul style="list-style-type: none"> c. Testing and documenting the effectiveness and potential side effects of available updates before installation; d. Ensuring that patches are installed in a timely manner; and e. Reviewing updates to ensure they are applied successfully. 	<p>Implemented at 6 months</p> <p>Implementation in process See explanation for Recommendation 1.2.</p> <p>Implemented at 6 months</p>
<p>1.3 The Department should develop and implement written policies and procedures for securely configuring IT systems. These policies and procedures should include:</p> <ul style="list-style-type: none"> 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; b. Developing and documenting baseline configurations for each IT system, as appropriate; c. Developing and documenting specific configuration settings; d. Ensuring default credentials are changed; and e. Defining the frequency of reviews and updates to the configurations. 	<p>The Department is acquiring software and updating written policies and procedures for managing IT system configurations. The Department has not yet begun addressing all of the recommendations in this area, but reported that it plans to implement all of them between July 2016 and January 2017.</p> <p>Implementation in process See explanation for Recommendation 1.3.</p> <p>Not implemented See explanation for Recommendation 1.3.</p> <p>Not implemented See explanation for Recommendation 1.3.</p> <p>Not implemented See explanation for Recommendation 1.3.</p> <p>Implementation in process See explanation for Recommendation 1.3.</p>
<p>1.4 The Department should improve management of access controls across IT systems. These improvements should include developing and implementing written policies and procedures for:</p> <ul style="list-style-type: none"> a. Reviewing file share rights, as appropriate, to ensure unnecessary access is not granted to users; b. Reviewing and adjusting, as needed, user access and account access privileges periodically; c. Ensuring appropriate separation between highly privileged accounts and standard user accounts; and d. Ensuring all passwords are changed on a regular basis, including establishing requirements and time frames for changing service account passwords. 	<p>The Department has generally not yet begun developing and implementing written policies and procedures to address the recommendations in this area, although it reported that it plans to do so by January 2017. The Department has implemented procedures to review some users' access.</p> <p>Not implemented See explanation for Recommendation 1.4.</p> <p>Implementation in process See explanation for Recommendation 1.4.</p> <p>Not implemented See explanation for Recommendation 1.4.</p> <p>Not implemented See explanation for Recommendation 1.4.</p>

Recommendation	Status/Additional Explanation
<p>1.5 The Department 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:</p> <ul style="list-style-type: none"> a. What IT systems and functions in each IT system should be logged; b. How frequently each log should be monitored; c. Who is responsible for ensuring logging occurs and reviewing logs on a regular basis; d. Standard response actions for possible detected events, including reporting the security status of the Department as a whole and information systems to critical personnel; and e. Provisions for log security and retention. 	<p>The Department is developing and implementing written policies and procedures that address the recommendations for log monitoring. Some of the recommendations have been implemented, and the Department reported that it plans to implement the remaining recommendations by January 2017.</p> <p>Implementation in process See explanation for Recommendation 1.5.</p> <p>Implementation in process See explanation for Recommendation 1.5.</p> <p>Implementation in process See explanation for Recommendation 1.5.</p> <p>Implemented at 6 months</p> <p>Implemented at 6 months</p>

Finding 2: Department should continue developing its information security program

<p>2.1 The Department should ensure that its ISO regularly monitors department-wide compliance with the information security program policies and procedures.</p>	<p>Implementation in process The Department has begun implementing software tools to monitor staff compliance with the information security program policies and procedures. The Department reported that it plans to implement updated policies and procedures for ensuring department-wide compliance by January 2017.</p>
<p>2.2 The Department 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 Department should:</p> <ul style="list-style-type: none"> 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; b. Establish written security agreements with the external organizations that require access to its information systems that outline information system connections' security requirements; 	<p>Not implemented The Department reported that it plans to implement this recommendation by January 2017.</p> <p>Implementation in process The Department is working to update and establish interconnection security agreements, which it reported that it plans to implement by January 2017.</p>

Recommendation

Status/Additional Explanation

- c. Develop and implement department-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;
- 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; and
- 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.

Implementation in process

The Department performs ad hoc risk assessments for some processes or systems but has not yet developed an annual formal risk assessment process. The Department reported that it plans to implement this process by January 2017.

Implementation in process

The Department has made progress in enhancing its security awareness education and training program but lacks provisions for role-based training and enhanced testing of staff susceptibility to social engineering attempts. The Department reported that it plans to fully implement this recommendation by January 2017.

Not implemented

The Department reported that it plans to implement this recommendation by January 2017.

- 2.3 The Department 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.

Implementation in process

The Department has taken steps to begin writing an action plan for the completion of its information security program and reported that it plans to fully implement this recommendation by January 2017.

Finding 3: Department has taken steps to ensure physical security of taxpayer information, but some improvements needed

- 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.

Implementation in process

The Department has finalized policies and procedures for annually reviewing badge access rights to sensitive areas. The Department anticipates completing its first annual badge access review using these procedures in July 2016.

- 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.

Implemented at 6 months

Recommendation**Status/Additional Explanation**

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.

Implementation in process

The Department's new employee training includes information on the clean-desk policy, and the Department is working to enhance its June 2016 recertification training, which all employees are required to take, to include more information about the policy. However, the Department has not yet developed or implemented additional written supervisory procedures for ensuring compliance 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 machines/printers.

Implemented at 6 months