MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

ARIZONA AUDITOR GENERAL
LINDSEY A. PERRY

JOSEPH D. MOORE
DEPUTY AUDITOR GENERAL

February 7, 2020

The Honorable Anthony Kern, Chair
Joint Legislative Audit Committee

The Honorable Rick Gray, Vice Chair
Joint Legislative Audit Committee

Dear Representative Kern and Senator Gray:

We have recently completed a 48-month followup of the Arizona Department of Revenue—Security of Taxpayer Information regarding the implementation status of the 36 audit recommendations (including subparts of the recommendations) presented in the performance audit report released in September 2015 (Auditor General Report No. 15-116). As the attached grid indicates:

- 23 have been implemented.
- 13 are in the process of being implemented.

Unless otherwise directed by the Joint Legislative Audit Committee, this concludes our follow-up work on the Department's efforts to implement the recommendations from the September 2015 performance audit. We will continue to assess the Department's IT security processes and practices as part of our annual financial audit work and report any issues we identify, as appropriate, in the State's annual single audit report.

Sincerely,
Dale Chapman, Director
Performance Audit Division

cc: Carlton Woodruff, Director
Arizona Department of Revenue

Arizona Department of Revenue—Security of Taxpayer Information
Auditor General Report No. 15-116
48-Month Follow-Up Report

Recommendation	Status/Additional Explanation
Finding 1: Department needs to improve its IT security	
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:	
a. Ensure all systems are included in vulnerability scanning, such as using automated tools to discover systems on the network;	**Implemented at 6 months**
b. Regularly conduct vulnerability assessments that determine whether security requirements and controls are functioning effectively;	**Implemented at 24 months**
c. Analyze vulnerabilities to determine their impact on systems and the associated risk;	**Implemented at 24 months**
d. Review and then remediate, based on risk, the problems identified during these vulnerability assessments;	**Implementation in process** The Department has implemented a written vulnerability-management policy for reviewing and remediating vulnerabilities based on risk. However, as reported in our prior followup, the Department does not always remediate vulnerabilities within the time frames specified in its policy. For example, although the policy states that critical vulnerabilities should be remediated within 10 days and high vulnerabilities within 30 days, we found that about 19 percent of the unique critical and high vulnerabilities the Department identified in August 2019 had not been remediated as of October 2019. The Department reported that it continues to work toward adhering to its time frames.
e. Accept the risk of weaknesses that cannot be mitigated; and	**Implemented at 24 months**
f. Assign roles and responsibilities to each task to ensure the process is performed in a timely manner.	**Implemented at 24 months**

Recommendation	Status/Additional Explanation
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:	
a. Determining and documenting whether or not a software or system update should be applied;	**Implemented at 24 months**
b. Addressing identified vulnerabilities, or accepting, justifying, and documenting the risk of not updating the software or system if there are extenuating circumstances;	**Implemented at 24 months**
c. Testing and documenting the effectiveness and potential side effects of available updates before installation;	**Implemented at 6 months**
d. Ensuring that patches are installed in a timely manner; and	**Implementation in process** Although the Department has an automated process to assist with installing patches, we identified patches that were not installed within the applicable time frames outlined in the Department's policy. The Department reported that it continues to work toward adhering to the time frames outlined in its policy.
e. Reviewing updates to ensure they are applied successfully.	**Implemented at 6 months**
1.3 The Department 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;	**Implementation in process** The Department has continued to configure its IT systems so that they do not provide more functionality than is necessary and has provisions and controls to ensure that unauthorized or unneeded software is not installed or used. However, the Department has yet to develop and implement formalized procedures for configuring all IT systems so they do not provide more functionality than is necessary. The Department reported that it plans to fully implement this recommendation by 2022.
b. Developing and documenting baseline configurations for each IT system, as appropriate;	**Implementation in process** The Department has continued to develop and document baseline configurations for its IT systems, with a focus on IT systems touching federal tax information data. However, the Department has yet to develop and document baseline configurations for all of its IT systems. The Department reported that it plans to fully implement this recommendation by 2022.

Recommendation	Status/Additional Explanation
c. Developing and documenting specific configuration settings;	**Implemented at 48 months**
d. Ensuring default credentials are changed; and	**Implemented at 36 months**
e. Defining the frequency of reviews and updates to the configurations.	**Implemented at 24 months**
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:	
a. Reviewing file share rights, as appropriate, to ensure unnecessary access is not granted to users;	**Implementation in process** The Department has documented procedures for its file-share-access-review process and continues to make efforts to review some file share rights. However, as reported in the prior followup, its policy does not include enough detail to illustrate how the Department plans to review file share rights, including who is responsible for reviewing file share rights. The Department reported that it continues to work on reviewing file share rights and plans to implement this recommendation by August 2020.
b. Reviewing and adjusting, as needed, user access and account access privileges periodically;	**Implemented at 24 months**
c. Ensuring appropriate separation between highly privileged accounts and standard user accounts; and	**Implementation in process** The Department has an access control policy that includes the appropriate separation between highly privileged accounts and standard user accounts and corrected the nonseparated accounts identified during the prior followup. However, we identified 12 user accounts in which both standard and privileged accounts had privileged access and 7 users who did not have a separate nonadministrative account. The Department reported it addressed the access for the 7 users and plans to continue improving its review process.

Recommendation	Status/Additional Explanation
d. Ensuring all passwords are changed on a regular basis, including establishing requirements and time frames for changing service account passwords.	**Implementation in process** The Department has a policy that requires service account passwords to be changed on a regular basis, but the policy does not require service account passwords to be changed when an individual who knows a password leaves the Department. In addition, the Department indicated that it has a process for changing service account passwords for some of its IT systems, but it has not yet established requirements for changing service account passwords for all of its IT systems. The Department stated it will need to conduct a Department-wide assessment to evaluate the impact of changing service account passwords on all IT systems and applications before service account passwords can be changed. The Department reported that it anticipates fully addressing this recommendation in fiscal year 2020.
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:	
a. What IT systems and functions in each IT system should be logged;	**Implementation in process** The Department has developed and begun to implement written policies and procedures for log monitoring critical activities that describe the IT systems and functions in each IT system that should be logged. However, the Department has yet to implement these policies and procedures across all of its IT systems. The Department reported it will fully implement this recommendation by August 2020.
b. How frequently each log should be monitored;	**Implemented at 24 months**
c. Who is responsible for ensuring logging occurs and reviewing logs on a regular basis;	**Implementation in process** The Department has defined teams who are responsible for ensuring logging occurs and reviewing logs on a regular basis; however, the Department's policies and procedures do not reflect this. The Department reported that it plans to update its policies and procedures by August 2020.
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	**Implemented at 6 months**
e. Provisions for log security and retention.	**Implemented at 6 months**
Finding 2: Department should continue developing its information security program	
2.1 The Department should ensure that its ISO regularly monitors Department-wide compliance with the information security program policies and procedures.	**Implemented at 36 months**

Recommendation	Status/Additional Explanation
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:	
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;	**Implementation in process** The Department has a data classification policy that is consistent with ASET requirements and a data classification procedure that is consistent with some ASET requirements, and it has begun inventorying some of its data. However, the procedure does not contain details for transmitting and processing sensitive data, and the Department has yet to complete its data inventory. The Department reported that it plans to continue to work on its data classification inventory to include all Department data.
b. Establish written security agreements with the external organizations that require access to its information systems that outline information system connections' security requirements;	**Implementation in process** The Department has developed a standard form for security agreements that sufficiently outlines the information system connections' security requirements and has used this form for one security agreement. The Department reported that it plans to implement the standard form for all of its new and existing security agreements by August 2020.
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;	**Implementation in process** The Department has a draft risk and data classification procedure that it uses to evaluate risks on IT projects. However, the draft procedure does not address Department-wide risk assessments consistent with ASET requirements. The Department indicated it is drafting a new risk assessment policy and procedure that will meet the ASET requirements for performing Department-wide risk assessments annually and documenting the results and potential impacts of the identified risks. The Department reported that it plans to fully implement this recommendation by March 2020.
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 emails or telephone calls and practical examples of phishing attacks to provide illustrations for employees; and	**Implemented at 24 months**

Recommendation	Status/Additional Explanation
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.	**Implemented at 36 months**
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 reported it is in the process of revising its Plan of Action and Milestones (POAM) for its information security program due to recent changes in Department leadership. The Department expects to update and fully implement its POAM by December 2020.
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.	**Implemented at 24 months**
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**
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.	**Implemented at 24 months**
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**