A REPORT
TO THE
ARIZONA LEGISLATURE

Performance Audit Division

Performance Audit

Arizona Department of Revenue

Department Should Improve Its Information Technology Security, Continue Developing Its Information Security Program, and Enhance the Physical Security of Taxpayer Information

September • 2015
Report No. 15-116

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

Debra K. Davenport
Auditor General

The **Auditor General** is appointed by the Joint Legislative Audit Committee, a bipartisan committee composed of five senators and five representatives. Her mission is to provide independent and impartial information and specific recommendations to improve the operations of state and local government entities. To this end, she provides financial audits and accounting services to the State and political subdivisions, investigates possible misuse of public monies, and conducts performance audits of school districts, state agencies, and the programs they administer.

The Joint Legislative Audit Committee

Senator **Judy Burges**, Chair

Senator **Nancy Barto**
Senator **Lupe Contreras**
Senator **David Farnsworth**
Senator **Lynne Pancrazi**
Senator **Andy Biggs** (*ex officio*)

Representative **John Allen,** Vice Chair

Representative **Regina Cobb**
Representative **Debbie McCune Davis**
Representative **Rebecca Rios**
Representative **Kelly Townsend**
Representative **David Gowan** (*ex officio*)

Audit Staff

Dale Chapman, Director

Jeremy Weber, Manager and Contact Person
Melinda Gardner, Manager
Brian Miele, Team Leader
Alex Entringer
Katie Morris
Nicole Palmisano
Nate Robb

The Auditor General's reports are available at:

www.azauditor.gov

Printed copies of our reports may be requested by contacting us at:

Office of the Auditor General
2910 N. 44th Street, Suite 410 • Phoenix, AZ 85018 • (602) 553-0333

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

September 30, 2015

Members of the Arizona Legislature

The Honorable Doug Ducey, Governor

Mr. David Raber, Director
Arizona Department of Revenue

Transmitted herewith is a report of the Auditor General, *A Performance Audit of the Arizona Department of Revenue—Security of Taxpayer Information*. This report is in response to an October 3, 2013, resolution of the Joint Legislative Audit Committee and was conducted as part of the sunset review process prescribed in Arizona Revised Statutes §41-2951 et seq. I am also transmitting within this report a copy of the Report Highlights for this audit to provide a quick summary for your convenience.

As outlined in its response, the Arizona Department of Revenue agrees with all of the findings and plans to implement all of the recommendations.

My staff and I will be pleased to discuss or clarify items in the report.

Sincerely,

Debbie Davenport
Auditor General

Attachment

2910 NORTH 44th STREET • SUITE 410 • PHOENIX, ARIZONA 85018 • (602) 553-0333 • FAX (602) 553-0051

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

Arizona Department of Revenue—Security of Taxpayer Information

REPORT HIGHLIGHTS
PERFORMANCE AUDIT

Our Conclusion

To perform its business functions, the Arizona Department of Revenue (Department) handles large volumes of both paper and electronic sensitive taxpayer information. The volume and nature of this sensitive information make the Department a potential target for attack by malicious individuals or organizations looking to access and/or steal this information. The Department has taken steps to protect taxpayer information; however, we identified vulnerabilities that leave taxpayer information at risk. In order to address these vulnerabilities, the Department should improve its information technology (IT) security, continue to develop its information security program, and enhance the physical security of taxpayer information.

2015

September • Report No. 15-116

Department needs to improve its IT security

Sensitive information and systems exposed because of IT security weaknesses—Security weaknesses can be exploited to gain access to and/or compromise IT systems, which can result in considerable costs to both organizations and individuals whose information is accessed. By simulating common attack patterns, we were able to gain unauthorized access to sensitive taxpayer information by exploiting weaknesses in the Department's internal IT systems. Through this effort, we found that we could take over user accounts that could be used to view, alter, or delete sensitive taxpayer information. We also performed successful social engineering techniques against department employees, which revealed weaknesses in some of the Department's controls and IT security training.

Improvements needed to Department's IT security processes—Although the Department has established various processes to help secure its IT systems, it needs to improve its IT security practices in several areas:

- **Documented processes needed for securely maintaining IT systems—**The Department has some processes for reviewing IT system vulnerabilities; applying patches, or updates and fixes, to systems; and configuring IT systems. However, the Department needs to document and/or enhance its policies and procedures in these areas.
- **Inadequate process for restricting access to only authorized users—**Although the Department performs some aspects of access control, we identified multiple deficiencies that provide department staff excessive access to information on the Department's IT systems, including some sensitive files not restricted on the Department's network, active user accounts that were unused or linked to terminated employees, and passwords that were older than allowed by department policy.
- **Insufficient IT system log monitoring—**Monitoring logs of critical IT system activities helps organizations track events on IT systems and networks and detect improper actions by any IT system user, whether staff or nonstaff. However, the Department performs only limited log monitoring.

Recommendations

The Department should:

- Develop and implement written policies and procedures to improve its vulnerability assessment processes, patch management, and configuration control;
- Improve management of access controls across IT systems; and
- Develop and implement a continuous log-monitoring program for critical IT activities.

Department should continue developing its information security program

Information security officer (ISO) position's authority strengthened—In January 2015, the Department enhanced the authority of its ISO position, which is responsible for overseeing department information security efforts. Although the ISO's responsibili-

ties are consistent with IT standards and best practices, the ISO has historically not overseen IT security for some IT systems managed by certain divisions. The Department should ensure the ISO regularly monitors department-wide compliance with information security program policies and procedures.

Department has begun developing information security program—Consistent with state requirements, the Department has begun developing an information security program by drafting additional information security policies. As of July 2015, the Department had drafted all of its policies but had not yet finalized some of them and had not yet developed most of the related procedures. For example, the Department lacked adequate procedures in four key security program areas we reviewed: data classification, risk assessment, information security awareness education and training, and incident response. IT standards and best practices recommend developing an action plan to guide the development and implementation of an information security program, which includes identifying tasks that need to be accomplished, the resources required to accomplish these tasks, and scheduled completion dates for the milestones established. Therefore, the Department should develop and implement an action plan and milestones to finish developing its information security program.

Recommendations

The Department should:

- Ensure the ISO position regularly monitors department-wide compliance with information security program policies and procedures; and
- Implement an action plan to complete the development of its information security program.

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

Department has taken steps to ensure physical security of taxpayer information—Because the Department keeps both paper and electronic taxpayer information in each of its four buildings, it is important that areas containing this information be secure. The Department uses several security measures, such as security guards and cameras, physical barriers, and badge access readers, to limit physical access to its buildings and taxpayer information. The Department also moved its tax-processing division out of its main building to an unmarked location that provides for enhanced security.

Additional measures needed to safeguard taxpayer information—We identified some areas where the Department's physical security can be strengthened. For example, although the Department requires badge access for employees to access most areas of its buildings, the Department did not document the destruction of employee badges when employees left the Department's employment. Additionally, not all badges were deactivated in a timely manner. We also found that, although the Department has a clean-desk policy requiring employees to secure any documents containing taxpayer information when they leave their workspace and a procedure regarding clearing off fax machines, employees did not always comply with this policy and procedure, sometimes leaving taxpayer information in plain sight. Additionally, there is no procedure for clearing sensitive information off copy machines/printers.

Recommendations

The Department should:

- Document its destruction of former employees' badges and ensure they are deactivated in a timely manner;
- Ensure employees comply with its clean-desk policy and fax machine procedure; and
- Expand the fax machine procedure to include copy machines/printers.

TABLE OF CONTENTS

TABLE OF CONTENTS

INTRODUCTION
Scope and Objectives

The Office of the Auditor General has conducted a performance audit of the Arizona Department of Revenue (Department)—Security of Taxpayer Information pursuant to an October 3, 2013, resolution of the Joint Legislative Audit Committee. This report is the second in a series of three reports conducted as part of the sunset review process prescribed in Arizona Revised Statutes 41-2951 et seq. It examines the effectiveness of department processes for safeguarding state taxpayer information.[1] The first report addressed the Department's use of information technology (IT) and its IT governance and management processes (see Report No. 15-105). The final report addresses the statutory sunset factors (see Report No. 15-117).

Department responsible for safeguarding taxpayer information

Department processes, uses, and stores large volumes of sensitive taxpayer information

The Department processes, uses, and stores large volumes of sensitive taxpayer information, in both paper and electronic formats, that it uses to administer the State's tax laws. Sensitive taxpayer information includes any information that identifies a taxpayer, such as a name, social security number, birthdate, or any banking, financial, or tax information. The Department uses this information to perform its core business functions, which include processing taxes, auditing taxpayers, collecting monies owed to the State, assisting taxpayers with questions, and performing economic analyses. The Department maintains this information for every taxpayer in Arizona, including individuals and businesses, and keeps this information for many years. For fiscal year 2015 alone, the Department received and processed more than 5.7 million tax documents from individuals and businesses containing sensitive taxpayer information.

Department's work makes it a target for potential attack

Although the Department's Chief Information Officer (CIO) reported that, to her knowledge, there have been no security breaches at the Department, the volume of sensitive information the Department maintains makes the agency a potential target for attacks by malicious individuals or organizations. The Department is responsible for safeguarding taxpayer information from attacks, including unauthorized access by department employees as well as threats from outside the agency. Safeguarding this information requires proper security of both paper and electronic taxpayer information.

In particular, proper IT security is vital to protecting the large amounts of electronic taxpayer information the Department uses. According to the Privacy Rights Clearinghouse, a nonprofit consumer education and advocacy organization dedicated to helping individuals protect their privacy, approximately 420 electronic data breaches were reported by government organizations and educational institutions in the United States between 2011 and 2014.

[1] The purpose of this audit was to examine how effectively the Department safeguards state taxpayer information. The Department also handles federal taxpayer information; however, the U.S. Internal Revenue Service (IRS) evaluates the security of this information.

Symantec, a well-known IT security company, reported that the number of breaches worldwide has increased 23 percent from 2013 to 2014.[1] These breaches have considerable costs to both organizations and individuals. Organizations must generally notify potential victims, may provide credit monitoring services to victims, may experience legal and other costs, and may lose public trust. Individuals who have information improperly accessed or stolen may spend time and resources monitoring their credit and may become victims of identity theft.

Department has taken steps to safeguard taxpayer information

The Department has taken several steps to help ensure the safety of taxpayer information. These include the following:

- **Employs information security staff—**The Department employs staff responsible for ensuring department IT systems and data are secure. The Department reported that it employs more than 50 staff in its IT division who perform information security functions, such as developing secure code for department applications, network engineering, and database administration. The Department has dedicated some of these employees exclusively to information security, including an Information Security Officer (ISO) and several information security staff. The Department reported that it spent approximately $5.5 million in fiscal year 2015 for information security, including staff, training, new equipment, and other expenses such as the encryption project described below.

- **Has begun development of information security program—**The Department has policies to help ensure the security of taxpayer information and has begun developing a more comprehensive set of security policies and procedures. As discussed in Finding 2, pages 15 through 22, these policies and procedures will comprise an information security program that is consistent with state-wide requirements imposed by the Arizona Strategic Enterprise Technology Office (ASET), which oversees IT in the State. The security program is being developed by the Department's Information Security Steering Committee, which comprises several staff, including the CIO and ISO.

- **Is enhancing existing data encryption—**The Department has been enhancing its data encryption technologies through an ongoing encryption project. This project involves upgrades to network firewalls to encrypt data as it moves throughout the Department's network, improvements to encryption for data that resides on network servers and storage devices, and enhanced encryption for staff workstations. When the project is completed, which the Department anticipates will be in December 2015, taxpayer information will be better protected should unauthorized access occur.

- **Performs background checks—**The Department reported that it performs criminal background checks for all of its full-time and part-time employees, contractors, and temporary employees.

[1] Symantec. (2015). *Internet Security Threat Report, Vol. 20*.

- **Ensures physical security of taxpayer information—**The Department has taken many measures to ensure the physical security of both electronic and paper taxpayer information. These measures include employing security guards; using tools like security cameras, metal detectors, and electronic badge readers; moving some operations to a more secure facility; and maintaining physical security policies (see Finding 3, pages 23 through 27, for additional information).

FINDING 1

Department needs to improve its IT security

The Arizona Department of Revenue (Department) should improve its information technology (IT) security controls to ensure that state taxpayer information is better protected from unauthorized access. Attacks on IT systems exploit IT weaknesses and can result in considerable costs to both organizations and individuals whose information is accessed. Although the Department has established various IT security controls and practices, the IT systems that auditors tested on the Department's internal network contained common security weaknesses that could allow unauthorized access to sensitive information, such as contents of tax returns, including social security numbers, or allow access to perform tasks, such as editing or destroying data. To better protect information in its internal network systems, the Department should improve its IT security practices by sufficiently reviewing vulnerabilities; documenting and following its process for applying patches, or updates and fixes, to its IT systems; more securely configuring its IT systems; ensuring proper management of access rights; and implementing structured log-monitoring practices.

Security attacks exploit IT weaknesses and can result in considerable costs

Security weaknesses can be exploited to gain access to and/or compromise IT systems, which could result in theft and/or loss of sensitive information. Although each security incident is unique, most attacks against an IT system follow a similar process. Subsequently, security testing activities generally try to mirror how an attack may be performed. In most instances, security attacks include the following three general steps:

1. **Public information gathering**—An attacker will attempt to gather as much information about an entity as possible using public resources, such as information available through the Internet, in order to focus attacks on weak points.

2. **IT system scanning**—An attacker will perform some direct probing steps to attempt to find weaknesses, such as scanning entity resources with automated tools.

3. **Exploitation**—An attacker will attempt to exploit weaknesses to obtain unauthorized access to an IT system.

These steps may be used both externally—outside of an entity's network or building—and internally—inside an entity's network—depending on the attacker, the attacker's ultimate goal, and the resources available. When performed with success, the steps may build on one another to allow an attacker to gain unauthorized access. Consequently, the steps are not always performed in the order listed above and may be performed multiple times during an attempt to gain access. Further, social engineering may also be used in tandem with these steps by convincing users to provide attackers with information or the means needed to access systems (see textbox, page 6).

As discussed in the Introduction (see page 2), successful attacks can result in considerable costs to both organizations and individuals whose information is accessed, such as costs associated with notifying potential victims, credit monitoring, legal proceedings, loss of public confidence, and identity theft. Some recent examples that illustrate the potential impact of security vulnerabilities include the following:

- In March 2012, hackers gained access to a Utah Department of Technology Services computer server that stored Medicaid and Children's Health Insurance Program claims data. Hackers accessed approximately

780,000 records. The Utah Department of Health offered free credit-monitoring services for 2 years to those impacted by the breach. According to the Utah Department of Health, in fiscal years 2012 and 2013, the State spent $2.75 million in response to the breach. In addition to the breach costs, as a precautionary measure, the Governor requested a security review for all state agencies at a cost of $1.3 million.

- In August 2012, attackers used a phishing e-mail to access 3.6 million tax records from the South Carolina Department of Revenue. In response, South Carolina provided free identity theft protection and credit monitoring to those who may have been impacted. In all, the South Carolina Budget and Control Board approved a $20.1 million loan to cover the costs associated with the breach.

- Between February and May 2015, criminals breached the U.S. Internal Revenue Service's (IRS) IT systems and were able to access tax information for more than 100,000 taxpayers by using social security numbers, birthdates, street addresses, and other personal information obtained elsewhere. The IRS reported that 200,000 taxpayers' accounts received suspicious login attempts, and half of those were successful. Additionally, the IRS will be providing credit-monitoring services to taxpayers affected by the breach.

Social engineering

Social engineering attacks attempt to persuade an entity's employees to provide some information about, or direct access to, the entity's network using devious means. Social engineering attacks may include:

- **E-mail phishing**—Sending devious e-mails in an attempt to convince a user to click on a link to open an external connection the attacker may use to gain unauthorized access.
- **Phone phishing**—Calling employees under false pretenses to persuade them to divulge sensitive information, such as personal information or their usernames and passwords.
- **Physical social engineering**—Attempting to convince employees at an entity to grant access to a physical building by playing a part or pretending to have the appropriate permission for access.

Source: Auditor General staff analysis of IT definitions from various sources.

Sensitive information and systems exposed because of Department's IT security weaknesses

By simulating common attack patterns, auditors were able to access sensitive taxpayer information by exploiting security weaknesses in the Department's core IT systems. Auditors' successful social engineering attacks also exposed weaknesses in the Department's IT security training.

Auditors gained access to sensitive information at the Department—Auditors were able to gain unauthorized access to sensitive taxpayer information by exploiting common weaknesses—weaknesses that are prevalent across many different organizations—in the Department's internal IT systems. Specifically, auditors were granted internal access to the Department's network to conduct automated testing on the Department's network and IT

systems to identify security weaknesses and vulnerabilities. Auditors then simulated processes to replicate what a malicious attacker could use to attempt to gain access to IT systems. Auditors subsequently reviewed these results to identify and successfully exploit several vulnerabilities that would have permitted access to sensitive information to any user connected to the Department's internal network. Based on this effort, auditors found that they could exploit an internal security weakness that allowed them to take over a large number of user accounts, including accounts with administrator access. These administrator accounts could be used to view, alter, or delete sensitive taxpayer information, including social security numbers, names, and addresses, for tax records dating back to at least 2007.

In addition, auditors identified weaknesses in the configuration of department computer and network resources. These weaknesses would have allowed auditors to control some of these resources and could have led to the theft and/or loss of sensitive data.

Auditors simulated successful social engineering attacks—Auditors performed a number of social engineering techniques that revealed weaknesses in some of the Department's controls and IT security training. Auditors were able to use social engineering to entice department employees to perform actions or provide information that could have been used by auditors to access their computers, network accounts, and the information to which those employees have access. Although some department controls intercepted or prevented some of auditors' attempts to access department computers and information, these controls could not successfully prevent all attempts. Similarly, the successful attack against the South Carolina Department of Revenue discussed previously was accomplished through social engineering. See Finding 2, pages 19 through 20, for auditors' recommendations for enhancing information security awareness education and training.

Department has various IT security processes but should take steps to improve them

Although the Department has established various processes to help secure its IT systems and taxpayer information, it needs to improve its IT security practices in several areas. These improvements include sufficiently reviewing vulnerabilities; documenting and following its process for applying patches, or updates and fixes, to systems; more securely configuring its IT systems; ensuring proper management of access rights; and implementing structured log-monitoring practices.

Processes needed for securely maintaining IT systems—The Department uses a number of security management processes to help secure its IT systems and help prevent the type of unauthorized access gained by auditors, but the processes need improvement. For example, the Department has developed some processes for vulnerability management, patch management, and configuration control; however, the Department should improve these processes to ensure it better secures IT systems. Specifically:

- **Documented vulnerability-management process needed—**The Department uses vulnerability management to help ensure IT system security. Vulnerability management is the process of identifying vulnerabilities such as IT security weaknesses, evaluating the

associated risks, and either correcting the vulnerabilities or documenting the acceptance of the risks. Although the Department performs vulnerability scans on a regular basis, it has not created a documented vulnerability management process to help ensure this process is performed with sufficient rigor and timeliness. Specifically, auditors found the following:

- **Not all IT systems scanned for vulnerabilities—**The Department scans most of its IT systems on a regular scheduled basis; however, the Department has historically neglected to include some IT systems in the vulnerability scans. As a result, department employees were unaware of these systems' security implications, as their statuses were never reported.

- **Numerous security vulnerabilities—**Auditors' review of the Department's network found that more than 85 percent of IT systems had critical, high, or medium vulnerabilities, some dating back to 2005. These vulnerabilities could potentially be used to gain unauthorized access to IT systems and sensitive information.

- **Vulnerabilities not sufficiently reviewed—**Despite the high volume of vulnerabilities in the Department's IT environment, the Department has not assigned sufficient resources to reviewing and remedying these vulnerabilities and, consequently, does not address issues in a timely manner. As of June 2015, the Department had assigned one individual, who has several other responsibilities, to review scan results for issues, resulting in limited time dedicated to the reviews.

- **No formal remediation process—**The Department does not have any structured and documented remediation process to address detected vulnerabilities or formally accept their associated risks, such as when business needs outweigh security requirements. As a result, issues are fixed only on an ad hoc basis, where individual issues may be assigned to different staff members depending on their availability. In addition, for issues that are not addressed, it is unclear whether the Department has accepted the risk or just not taken action. This ad hoc process increases the Department's risk for IT system compromise and could lead to unauthorized disclosure of sensitive taxpayer information.

To improve its vulnerability management process, the Department should develop and implement written procedures for structured vulnerability assessments of its IT infrastructure. These procedures should include ensuring all systems are included in vulnerability scanning, such as using automated tools to discover systems on the network; regularly conducting vulnerability assessments that determine whether security requirements and controls are functioning effectively; analyzing vulnerabilities to determine their impact on systems and the associated risk; reviewing and then remediating, based on risk, the problems identified during these vulnerability assessments; accepting the risk of weaknesses that cannot be mitigated; and assigning roles and responsibilities to each task to ensure the process is performed in a timely manner. The Department should also complete the implementation of its information security program policy to help ensure all requirements regarding vulnerability scanning are performed appropriately (see Finding 2, pages 15 through 22, for additional details on the information security program). These

changes would assist the Department in identifying and addressing critical vulnerabilities in a timely manner and reduce the risk of data breach or data loss.

- **Documented patch management process needed—**Patch management is another important process for ensuring IT system security. Hardware and software vendors periodically issue updates, or patches, to their products to correct security vulnerabilities and other bugs that have been identified and to improve usability and performance. The process of reviewing updates, establishing a plan to apply them, and applying them, as appropriate, is referred to as patch management. Although the Department performs patch installations on its IT systems, it does not have a documented process for determining whether an IT system requires an update to mitigate a vulnerability. As a result, patching is done inconsistently, and many of its IT systems are not fully updated. Specifically, auditors discovered that updates had been available for several years for more than 50 percent of the Department's IT systems with vulnerabilities.

  To improve its patch management process, 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:

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

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

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

  - Ensuring that patches are installed in a timely manner; and

  - Reviewing updates to ensure they are applied successfully.

- **Documented process for securely configuring IT systems needed—**The Department does not review the configurations of network servers and other critical network resources to ensure that they are as secure as possible. Configurations are settings that control how systems operate, such as installed software and security protocols. Network servers and other devices, such as storage systems, provide and hold a significant portion of the critical functionality and sensitive information department employees need to complete their job duties. When IT systems are not properly configured, data those systems handle is more susceptible during attacks. For example, a configuration error at the Utah Department of Technology Services allowed hackers to bypass the security system and gain access to sensitive information, as discussed previously (see pages 5 through 6).

  Further, the Department has improper server configurations and unnecessary services and applications enabled on IT systems, which unnecessarily expose servers to risks that could

lead to exposure of sensitive information. Specifically, auditors found that department employees had installed software on servers that is typically required only on user workstations. Some of this software contained vulnerabilities. In addition, employees had not performed some configuration changes necessary to mitigate certain vulnerabilities that cannot be resolved by installing a patch.

Finally, default credentials were present on some systems and applications. Default credentials are paired sets of usernames and passwords, which are shipped with software and devices from the manufacturer, typically at the time of purchase. These credentials provide users with administrator rights for initial setup and configuration of IT systems. Part of this setup process would typically involve changing these default passwords to prevent attackers from using these credentials to gain access to IT systems.

To address these issues, the Department should develop and implement written policies and procedures for securely configuring IT systems. These policies and procedures should include 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; developing and documenting baseline configurations for each IT system, as appropriate; developing and documenting specific configuration settings; ensuring default credentials are changed; and defining the frequency of reviews and updates to the configurations.

Inadequate process for restricting access to only authorized users—Access control is critical to IT security in any organization. Access control is the process of granting or denying specific requests for obtaining and using information and related information-processing systems or services, or entering specific physical facilities.[1,2] Although the Department performs some aspects of access control, auditors identified multiple deficiencies that provide excessive access to information on the Department's IT systems. Specifically:

- **Some sensitive files not restricted on the network—**The Department does not always appropriately restrict access to sensitive files and information. For instance, when reviewing select files' access rights on the network, auditors found some file share folders that permitted nearly all network users inappropriate access to the files. These files included tax returns containing taxpayer information such as social security numbers, names, and addresses, which only some employees need access to in order to perform their duties. According to the Department, file share access is not reviewed regularly. Therefore, the Department should develop and implement written policies and procedures for reviewing file share rights, as appropriate, to ensure unnecessary access is not granted to users.

- **Terminated and unused accounts with active access to IT systems—**The Department does not have a process for reviewing user access on a regular basis or ensuring that employee access to IT systems is terminated upon employee separation from the Department. Auditors' review of various IT systems throughout the Department found

[1] Committee on National Security Systems. (2010). *National information assurance glossary*.

[2] This finding addresses access to IT systems. See Finding 3, pages 23 through 27, for information about the Department's security measures related to access to its physical facilities.

numerous active accounts that were either unused or linked to terminated employees. In addition, auditors found that access for most of the Department's IT systems is not reviewed on a periodic basis for changes and discrepancies. By not reviewing access periodically, the Department runs the risk of not detecting improper access to its systems in a timely manner, which could result in extended periods of unauthorized access to sensitive taxpayer information. In order to ensure the access-removal process is completed, the Department should develop and implement written policies and procedures for reviewing and adjusting, as needed, user access and account access privileges periodically.

- **Improper separation of administrator and standard accounts—**As of June 29, 2015, the Department had improperly separated some of its active domain administrator accounts—which are accounts that provide full control over most systems within an organization's network—from standard accounts. Because domain administrator accounts should be used for only limited actions on specific IT systems in a network, the Department opted to require that individuals who need to perform these types of actions have dual accounts, one that allows these types of activities and one that provides them with standard user access to the Department's network. Despite this design, auditors found that some of the standard user accounts also had administrator privileges. Consequently, these users always had administrator rights regardless of which account they used, thus increasing the risk to the Department if one of these standard user accounts were to be compromised. Further, this risk is increased because the Department does not regularly perform a review of its accounts, as discussed in the prior bullet. Therefore, in addition to developing and implementing written policies and procedures for reviewing user access and account privileges periodically, the Department should ensure that its highly privileged accounts are separated from standard user accounts.

- **Some passwords not changed often enough—**As of December 2014, the Department had numerous accounts with passwords that were older than 60 days, contrary to department password policy. The majority of these accounts were service accounts—privileged accounts used directly by computer systems to administer or operate functions or applications—although some belonged to individuals. Service accounts are often on a different password age schedule than employee accounts; however, the Department does not have a defined password expiration schedule for these accounts, and most of them had passwords older than 1 year. Consequently, any person who has prior knowledge of these account passwords may still have access to them, and any malicious user who gains access to such credentials may have extended access to the corresponding system. In addition, the Department has no process to evaluate the need to change these passwords based on the separation of individuals who would have known them from department employment. Therefore, the Department should develop and implement written policies and procedures that establish requirements and time frames for changing service account passwords, and ensure that all passwords are changed on a regular basis.

Insufficient IT system log monitoring—The Department has not adequately monitored the logs that capture information for its IT systems' user and computer activities. Monitoring logs of critical IT system activities enables organizations to track events on IT systems and networks and to detect improper actions by any IT system user, whether staff or nonstaff. These activities may include logins and connections to critical applications, systems, and devices, as well as changes

to data and data transfer activities. For example, the Department could monitor the bandwidth logs on its network to detect large data transfers, which may indicate data being sent out of the network without approval. The Department performs only limited log-monitoring efforts and, as a result, may not detect malicious or inappropriate activities on its IT systems.

To improve its log-monitoring efforts, 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 what IT systems and functions in each IT system should be logged; how frequently each log should be monitored; who is responsible for ensuring logging occurs and reviewing logs on a regular basis; 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 provisions for log security and retention.

Recommendations:

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;

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

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

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

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

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

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;

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

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.

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;

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.

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;

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.

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;

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.

FINDING 2

The Arizona Department of Revenue (Department) is taking steps to enhance information technology (IT) security department-wide, but additional action is needed to ensure that IT systems are adequately protected. Specifically, although the Department has strengthened the authority of its information security officer (ISO) position, which is responsible for directing and coordinating department information security efforts, it should ensure that the ISO regularly monitors department-wide compliance with security policies and procedures. Additionally, the Department has begun developing an information security program that is consistent with state requirements by drafting additional information security policies. As of July 2015, the Department had drafted but not finalized all of its policies, and had not yet developed most of the related procedures. For example, the Department lacked adequate procedures in four key security program areas auditors reviewed: data classification, risk assessment, information security awareness education and training, and incident response. Therefore, the Department should develop and implement an action plan and milestones to finish developing this program, including finalizing all of the policies and developing and implementing related procedures.

Department should continue developing its information security program

Information security officer's authority strengthened

In January 2015, the Department took a key step toward ensuring that sensitive information and systems are adequately protected by enhancing the authority of its ISO position, which is responsible for overseeing information security efforts at the Department. The Department had an ISO position as early as 2006, but the position did not have the full breadth of authority that the position now has. For example, although the ISO has always been responsible for participating in establishing security guidelines and policies, the January 2015 updated position description provided the ISO with the final authority to implement these guidelines and policies after department leadership approves them. In addition, the updated ISO position description specifies that the ISO has the authority to direct and coordinate all information security efforts department-wide, including establishing a department-wide information security program. As now defined, the ISO's documented responsibilities are consistent with IT standards and best practices that indicate there should be an individual who has sufficient authority over information security efforts organization-wide and is responsible for implementing the information security program.[1]

Although the ISO's documented responsibilities are consistent with IT standards and best practices, in practice, the ISO has not overseen all aspects of IT security department-wide. Specifically, the Department's ISO has historically not overseen IT security in some IT systems managed by certain divisions. The Department indicated that IT staff in these divisions had not coordinated IT security efforts with the ISO and his staff, such as the process to grant users with specific types of access and the process to document modifications to IT systems not managed by the IT division. As discussed on pages 16 through 17, the Department has begun enhancing its security policies as directed by state-wide requirements, which will help ensure the ISO position oversees all aspects of IT security department-wide. The Department should also ensure that its ISO regularly monitors department-wide compliance with the information security program policies and procedures.

[1] Ross, R., et al. (2013). *NIST Special Publication 800-53 Revision 4: Security and privacy controls for federal information systems and organizations.* Gaithersburg, MD: National Institute of Standards and Technology.

Department has begun enhancing its existing security policies by developing information security program

The Department has begun enhancing its existing security policies by developing an information security program in accordance with state-wide policy requirements. These requirements are based on IT standards and best practices, which recommend formalizing an information security program addressing areas such as data classification, risk assessment, information security awareness education and training, and incident response.

Best practices recommend a formalized information security program—IT standards and best practices indicate that to provide effective management direction and support for information security, the information security program should be formalized into an agency-wide written plan that identifies a governance structure, or the method by which information security will be directed, administered, and/or controlled.[1] They also indicate that the plan should be disseminated and communicated to appropriate persons. In addition, the Department was required to develop an information security program consistent with a state-wide policy implemented by the Arizona Department of Administration, Arizona Strategic Enterprise Technology Office (ASET). The policy required all state agencies' information security programs, including the Department's, to have draft policies by July 2015 that address 17 security areas based on IT standards and best practices.[2] Four key areas of an information security program reviewed in this audit are data classification, risk assessment, information security awareness education and training, and incident response (see textbox).

Four key areas of an information security program

- **Data classification**—The process of labeling information to show its level of sensitivity or the degree of protection needed when handling the information.
- **Risk assessment**—The process of identifying risks such as threats and vulnerabilities, determining the probability of their occurrence and the resulting impact, and identifying the additional security controls that would lessen this impact.
- **Information security awareness education and training**—Actions taken to regularly inform and train staff about information security risks and their responsibility to comply with policies to reduce these risks.
- **Incident response**—Procedures for detecting, reporting, and responding to information security incidents, such as a breach of confidential information due to a failure of IT security safeguards or computer hacking.

Source: Auditor General staff analysis of IT standards and best practices: ISO, 2005; and Ross et al., 2013.

Department has started developing information security program—To further enhance its existing security policies, the Department has begun developing an information security program that conforms to ASET's requirements. Although the Department previously

[1] International Organization for Standardization. (2005). *Information Technology—Security techniques—Code of practice for information security management*, (2nd ed.). Geneva, Switzerland; and Ross et al., 2013.

[2] The security areas are based on several IT standards and best practices, such as Ross et al., 2013, and PCI Security Standards Council. (2010). *Payment card industry data security standard: Requirements and security assessment procedures, version 2.0*.

had security policies, the policies did not include the level of detail or cover all of the subject areas ASET required. To assist state agencies in developing information security programs, ASET provided security policy templates for state agencies to adapt to their circumstances. The Department has an Information Security Steering Committee that it reported met regularly to discuss and draft these policies based on the ASET templates, and submit them to department leadership for approval. As of July 2015, the Department had completed drafts of the security policies ASET required, but department leadership had not finalized and approved 7 of the 17 policies. Additionally, the Department had not yet developed most of the supplemental procedures that specifically explain how the Department will implement the 17 policies, including procedures for the four key policy areas discussed in the next section.

Department should continue to establish information security program in four key areas

Although the Department has drafted all of the state-required policies for its information security program, one policy was lacking, and it had yet to develop most of its procedures in the four key information security program areas auditors reviewed. These four areas were data classification, risk assessments, information security awareness education and training, and incident response. The Department should continue to develop and implement its information security program consistent with state requirements in these four areas.

Department should establish data-classification procedures—The Department should create procedures to classify its data. According to IT standards and best practices, a data-classification process is critical to help ensure that sensitive data is identified and then protected based on risk, as well as to prevent unauthorized data access, modification, disclosure, or destruction.[1] Additionally, data classification would help the Department ensure that it meets requirements from the U.S. Internal Revenue Service regarding the privacy of federal taxpayer information. IT standards and best practices indicate that data classification should include an overall classification process (see textbox).

Data-classification process criteria

An organization-wide data-classification process should be established that:

- Protects information based on requirements such as confidentiality;
- Is reviewed and updated regularly; and
- Consists of an inventory of information classification details that includes classification, identity of the information owner, and a brief description of information classified.

Source: Auditor General staff analysis of IT standards and best practices: ISO, 2005; and Ross et al., 2013.

The Department created and approved a data-classification policy in December 2014 that is consistent with ASET requirements. However, the Department has not yet created procedures to implement its data-classification policy. Specifically, the Department has not inventoried and classified all of the data that it processes and stores, nor has it developed procedures for how it would do this.

[1] ISO, 2005; and Ross et al., 2013.

Additionally, without procedures to inventory and classify its data, the Department is unable to create written agreements that specify security requirements for external entities—such as local governments and businesses—that legitimately access its network. According to IT standards and best practices, these agreements should outline security requirements and the nature of information communicated to ensure the security responsibilities of both entities are addressed.[1] By not classifying its data, the Department runs the risk of providing external entities with access to data and information they do not need and/or should not have. Therefore, the Department should develop and implement procedures for the data-classification process that are consistent with ASET requirements, such as protecting the information based on confidentiality, and developing a data-classification inventory that is updated regularly. Further, the Department should establish written security agreements with external organizations that require access to its information systems that outline security requirements for these connections.

Department should develop IT risk assessment procedures—The Department has not yet adequately implemented IT risk assessments, another key area of an information security program, and should do so. According to IT standards and best practices, risk assessments are used in part to identify vulnerabilities within the organization, such as weak passwords, outdated systems, or lack of a plan for restoring IT or other business operations following a disaster, and to determine what controls are needed to lessen the risk of someone exploiting those vulnerabilities.[2] Risk assessments are also used to identify threats that originate outside of the Department. IT standards and best practices state that there should be documented policies and procedures for performing IT risk assessments that apply department-wide and mandate that they be regularly performed (see textbox).

Risk assessment criteria

A documented organization-wide risk assessment process should be established that:

- Assigns responsibility;
- Mandates regular assessments;
- Consists of a structured methodology for assessing risks, including control weaknesses and operating/environmental threats;
- Documents results and potential impact of risks;
- Uses results to make changes to the security program and address risks; and
- Reports results to top management.

Source: Auditor General staff analysis of IT standards and best practices: ISO, 2005; Ross et al., 2012; and Ross et al., 2013.

Without an effective risk analysis and assessment process, the Department may not adequately protect sensitive information or critical IT systems or infrastructure by avoiding or reducing security threats, such as computer-assisted fraud, vandalism, and fire or flood. The Department may also be unable to identify the controls needed to protect against threats to sensitive data, such as malicious code, which is computer code that has been written to deliberately perform unauthorized functions, or computer hacking, which is attempts to gain unauthorized access

[1] ISO, 2005; and Ross et al., 2013.

[2] ISO, 2005; and Ross, R., et al. (2012). *NIST Special Publication 800-30 Revision 1: Guide for conducting risk assessments*. Gaithersburg, MD: National Institute of Standards and Technology.

to computer systems for the purpose of stealing and corrupting data (see Finding 1, pages 5 through 6, for additional information about security attacks).

The Department approved a risk assessment policy in May 2015 as part of the overall information security program; however, procedures have yet to be developed and implemented for performing regular assessments. Although the Department performed an IT risk assessment in 2014, it last performed such an assessment in 2010. Therefore, the Department should continue its efforts to 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.

Department should enhance information security awareness education and training—Information security awareness education and training is critical to help detect and avoid information security problems and incidents. IT standards and best practices indicate that there should be a documented information security awareness education and training program (or set of activities) that is mandatory for all individuals who have access to the organization's information and systems (see textbox). Without an effective information security awareness program, the Department may not adequately inform staff of common and emerging information security threats and concerns as well as their responsibilities and liabilities related to these threats, or ensure its staff are equipped to support the Department's security policy in the course of their normal work.

Information security awareness education and training criteria

A documented organization-wide information security awareness education and training program consists of the following:

- Awareness or training activities for all individuals with access to the organization's information or systems;
- Is geared toward the individual's role;
- Is mandatory and kept up to date; and
- Provides information that helps individuals understand (a) the meaning of information security, (b) the importance of complying with information security policies, and (c) their responsibilities for information security (e.g., reporting actual and suspected incidents).

Source: Auditor General staff analysis of IT standards and best practices: ISO, 2005; and Ross et al., 2013.

The Department approved an information security awareness training and education policy in January 2015, but has yet to implement all processes outlined in the policy. Although the Department performs many activities related to information security awareness training, it has not developed mandatory information security awareness education and training that is specifically geared toward an individual's role within the Department, as ASET requires. For example, the Department requires all newly hired staff to attend training about unauthorized tax viewing, distributes a monthly newsletter regarding information security awareness topics, and provides training, as part of an annual recertification process for all staff, regarding IT policies. However, this training and other resources lack components ASET requires, such as detailed guidance for staff regarding phishing attacks and other common attack methods. Weaknesses in the Department's current training efforts may have contributed to auditors' successful social engineering attacks, as reported in Finding 1 (see page 7). Specifically, if employees were trained regularly on the most up-to-date common attack methods and how to respond, they may not have been as susceptible to auditors' social-engineering attacks.

Therefore, the Department should take additional steps to enhance its department-wide 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 specific 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.

Department should improve incident response policy and develop additional procedures—The Department should continue its efforts to develop and implement its incident response policy and additional procedures to ensure that information security events are reported and responded to as quickly as possible. According to IT standards and best practices, incident response is a process of detecting, reporting, and responding to information security incidents, such as a breach involving confidential information (see textbox). In addition, effective incident response reduces the risk of these incidents occurring, minimizes their overall impact, and ensures that legal requirements are followed if a security breach occurs. For example, Arizona Revised Statutes §44-7501 requires that any person or entity in Arizona holding computerized personal data should notify all affected parties if they determine there has been a security breach in which unauthorized access to unredacted or unencrypted personal information has occurred.

Incident response criteria

A standardized, documented, organization-wide process for managing information security incidents should be established that:

- Identifies roles and responsibilities;
- Provides the responding individuals with the authority to make critical decisions; and
- Provides information on how to identify, respond to, recover from, and follow up on information security incidents.

Source: Auditor General staff analysis of IT standards and best practices: ISO, 2005; and Ross et al., 2013.

The Department established an incident-response-planning policy in December 2014 and, in June 2015, developed one of its required procedures regarding privacy incident response.[1] However, the Department lacks a comprehensive incident response plan that provides staff with detailed procedures to follow in response to an incident. Additionally, although the Department's incident-response-planning policy meets most ASET requirements, the policy is missing some components. Specifically, the policy lacks guidance related to automated processes for handling and reporting incidents, and an area recommended by IT standards and best practices related to an information spillage response.[2,3,4] Further, the Department has not developed procedures for its newly approved incident-response-planning policy

[1] A privacy incident response procedure provides an organized approach to respond to security incidents involving unauthorized access to personally identifiable information. (Ross et al., 2013)

[2] Ross et al., 2013.

[3] Automated incident response processes can include incident management systems for handling incidents, and automated notifications or e-mails for reporting incidents. (Ross et al., 2013)

[4] Information spillage is a security incident that occurs whenever classified data is transferred to unaccredited or unauthorized systems, applications, or computer media, such as portable storage devices. (National Security Agency. (2012). *Securing data and handling spillage events*. Washington, DC.)

related to incident response training, testing, and monitoring. Therefore, the Department should improve its incident-response-planning policy and procedures to include automated processes and an information spillage response, then develop and approve an incident response plan.

Department should create action plan to complete development of its information security program

The Department should create an action plan to guide its efforts to complete the development of its information security program in a timely manner. ASET required state agencies to complete drafts of the policies in their information security programs for the 17 required areas by July 1, 2015. As stated previously, although the Department completed all of its draft policies by July 2015, it had not finalized and approved 7 of the 17 policies and had not yet developed most of the related procedures. IT standards and best practices recommend developing an action plan to guide the development and implementation of an information security program, which includes identifying tasks that need to be accomplished, the resources required to accomplish these tasks, and scheduled completion dates for the milestones established.[1] Although the Department has a process for drafting policies and procedures through its Information Security Steering Committee, it lacks a written action plan and milestones to complete the development of its information security program. Therefore, the Department should follow IT standards and best practices to develop and implement an action plan and milestones to ensure it completes the development of its security program in a timely manner.

Recommendations:

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

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;

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

[1] ISO, 2005; and Ross et al., 2013.

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.

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.

FINDING 3

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

The Arizona Department of Revenue (Department) has taken steps to ensure the physical security of taxpayer information, but can enhance some of its efforts. Proper physical security is necessary to protect both paper and electronic taxpayer information from unauthorized access. Whether paper or electronic, taxpayer information should not be accessed by department employees with no work-related reason to view the information or by any unauthorized person who may attempt to gain access to the information. The Department physically safeguards this information using a variety of measures, including security guards and cameras, maintaining barriers between publicly accessible and secure areas, controlling building access through electronic badge readers, and moving certain department functions to a more secure facility. However, the Department should document its destruction of former employees' badges and ensure they are deactivated in a timely manner. Additionally, the Department requires employees to assist in limiting access to taxpayer information by following certain policies. Auditors found that although some employees follow these policies, there is room for improvement.

Department limits access to areas where taxpayer information is stored

The Department uses several security measures to limit physical access to taxpayer information, including paper and electronic information. The Department uses and maintains both paper and electronic taxpayer information in each of its four buildings. As a result, it is important that areas containing this information be secure from both department employees who could improperly access that information through their work and others who could attempt to gain access to this information. The Department's security measures for limiting physical access include the following:

- **Employing security guards and using security cameras and metal detectors to protect buildings and information—**The Department posts contracted security guards at three of its four buildings. According to the Department, the fourth building is housed in a state complex and is secured by the Arizona Department of Public Safety's Capitol Police. At the Department's main Phoenix location, where taxpayers regularly conduct business in person, guards patrol entrances, screen visitors using metal detectors, and ensure that the public remains in designated areas. The Department also maintains security cameras at each of its locations. These cameras are monitored by guards and/or department staff.

- **Maintaining barriers between publicly accessible and secure areas—**Department buildings have areas that are accessible to the public. These areas allow the public to interact with department staff and conduct necessary business. However, the Department has physical barriers like electronic badge readers to prevent members of the public from entering secure areas (see the following bullet for more information on electronic badge access).

  Auditors performed numerous observations of the Department's main Phoenix location and did not observe any instances of visitors improperly accessing secure areas. Auditors also observed that the Department did not store any taxpayer information in publicly accessible areas. Department officials reported that the Department does not allow taxpayer information to be stored in publicly accessible areas at any of its locations.

- **Requiring badge access, although some procedures could be enhanced—**All employees, visitors, contractors, and temporary employees at the Department are required to wear badges. Requiring badges in this manner provides security for taxpayer information. Specifically:

  - **Badges indicate to security guards and other staff that the individual wearing the badge is authorized to be on the premises—**Guards and employees are instructed to look for badges as an indication that an individual is authorized to access the building. In numerous observations, auditors noted that department employees wore their badges appropriately. Additionally, employees were careful to ensure that auditors were wearing badges.

  - **Badges are electronically coded to grant access to different areas within the Department's buildings—**Badges are electronically coded to grant the wearer access to various department areas. At the Department's main Phoenix location, a typical employee would need to use his/her badge at least twice to access his/her work area. The Department can also use badges to limit employee access to only those buildings where access is necessary. For example, an employee who works at the Department's main Phoenix location would not be able to use his/her badge to access the Department's separate process administration building.

    Because some areas of the Department, like the server room, are especially sensitive, the Department requires additional security to ensure access is appropriate.[1] This means that only individuals whose job function requires they work in sensitive areas have access to these areas. For example, it would not be necessary for an employee who answers customer phone calls to access the server room, so his/her badge would not be coded to allow access to the server room. Auditors reviewed employees with badge access to the server room and concluded that their access was appropriate. Additionally, during the course of the audit, the Department reported that it was developing policies to annually review employee access to sensitive areas to ensure that all access remains appropriate. A department official also reported that whenever an individual with access to a sensitive area leaves the Department or changes job functions, or when a new employee requires this access, officials review the access list for everyone with this special access. The Department should continue to develop and implement these new policies for badge access to sensitive areas.

  Although requiring badge access to enter the Department's buildings limits access to taxpayer information, the Department should document compliance with its badge destruction and deactivation procedures and enhance its procedures in one area to help ensure that former employees are not able to access the Department. Department procedures require it to collect and shred former employees' badges; however, the Department does not document this process. As a result, it is not able to verify that all former employee badges are collected and shredded. In addition, the Department is also responsible for working with the Arizona Department of Administration (ADOA) to deactivate these badges. The ADOA handles coding and deactivating badges for most of

[1] The server room houses critical computer equipment.

the Department's badges.[1] Department procedures require that, when an employee leaves the Department, it request that ADOA deactivate the employee's badge. However, not all badges auditors reviewed were deactivated in a timely manner. As of May 6, 2015, auditors found that access had not been revoked for approximately 35 percent of employees who left the Department between January 1, 2014 and May 1, 2015. Although the Department reported that it requests badges to be deactivated immediately, it did not maintain documentation of these requests.

The ADOA plans to install a new security/access control system in ADOA-managed buildings in 2015. According to an ADOA official, this system will improve badge access security as it will require all tenants in ADOA-managed space to review their building access and will allow the ADOA to compare reports from the State's human resources software with agency access lists. In the meantime, 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.

- **Moving the tax-return-processing division to a more secure, unmarked location and providing for the secure transport of hard copy documents—**The Department's largest volume of paper and electronic taxpayer information flows through the Process Administration Division. This division processes all paper and electronic tax returns, as well as some additional tax documents. The division was previously located on multiple floors in the Department's main Phoenix location. As a result, hundreds of department employees had access to the division, and paper tax documents were moved around the building as part of day-to-day operations. Moving tax documents throughout a multi-floor building created additional risk of those documents becoming lost or inappropriately accessed. Housing the division in the Department's main office also increased the risk of unauthorized access because the location is well known and frequently visited by the public. To mitigate these risks and provide increased efficiency in document processing, the Department moved its Process Administration Division to a separate, single-floor, unmarked location that is accessible only to division employees. This has provided additional security to both paper and electronic taxpayer information processed at that location.

  Additionally, in order to process tax documents, the Process Administration Division sends documents for certain tax types to an offsite vendor to scan and image paper-filed returns. Vendor employees providing this service are required to undergo background checks. Additionally, the Department has performed occasional reviews of the imaging vendor to check for security vulnerabilities. The Process Administration Division uses computer programs to track where batches of documents are in the process and reported that no documents have been lost. Auditors observed division staff preparing documents and taking them to the imaging vendor and did not identify any security problems.

[1] The Department codes and deactivates badges used at the Department's Mesa location and Process Administration Division. This means that, for Mesa and process administration employees, the Department does not require the ADOA to deactivate employee badge access.

Department employees need to better protect taxpayer information

The Department maintains policies and procedures to help ensure that employees protect taxpayer information, but implementation of some of these policies should be improved. These policies require that employees take specific actions to protect taxpayer information. These include:

- **Shredding sensitive information (no needed improvements were identified)—**The Department requires that employees who wish to dispose of documents containing taxpayer information place these documents in locked shred boxes. Auditors observed numerous instances of employees complying with this policy.

- **Keeping desks clear of taxpayer information (improvements needed)—**The Department has a clean-desk policy that requires employees who are handling taxpayer information to remove this information from plain sight when they leave their desks for more than a few minutes. This includes locking away any documents containing taxpayer information and locking their computer screen so tax information is not visible. The policy also requires each department division to designate staff to inspect work areas at the end of each day to ensure that no taxpayer information is left out. The Department reported that it performs an annual after-hours inspection for compliance with this policy at its main Phoenix and Tucson locations.[1] The Department reported that, during an inspection, it will review any part of a building where confidential information is stored. According to the Department's Disclosure Officer, employees are not given notice of when an inspection will occur, and when a violation is found, she works to establish a corrective action plan, discusses the violation with division management, and often requires employees to receive additional training on the policy.

  Auditors performed numerous tests of this clean-desk policy and found that staff in the Process Administration Division, which handles the largest volume of taxpayer information, consistently complied with the policy. However, in other department divisions that regularly handle taxpayer information, auditors observed numerous policy violations. For example, in one division, an employee stepped away from his/her desk leaving numerous taxpayer checks with banking information and other sensitive documents out in the open for at least 20 minutes. Auditors also found this employee's desk drawers were left open with taxpayer files visible. In another division, an employee left his desk without locking his computer screen so taxpayer information was visible to anyone who walked by. Although the Department reported that all employees receive training and a copy of the clean-desk policy, the Department should implement additional training and supervision as needed to ensure compliance with this policy.

- **Clearing off copy machines, printers, and fax machines (improvements needed)—**Auditors noted multiple instances of documents containing sensitive taxpayer information being left for several minutes on fax machines and copy machines/printers. In June 2015,

[1] The Department reported that it does not perform similar inspections at the Washington Park or Mesa locations because there is less risk at these locations.

the Department developed a department-wide procedure for sending and receiving sensitive information on fax machines. For example, the procedure requires department employees who know they will be receiving a fax that contains sensitive information to promptly pick up the document from the fax machine. Additionally, the procedure requires department employees to periodically check fax machines to ensure that sensitive data is not left out. The Department should educate employees on this procedure. In addition, the Department should expand the procedure regarding fax machines to include copy machines/printers.

Recommendations:

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.

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.

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.

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.

APPENDIX A

Methodology

This appendix provides information on the methods auditors used to meet the audit objectives.

This performance audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The Auditor General and staff express appreciation to the Arizona Department of Revenue (Department) Director and staff for their cooperation and assistance throughout the audit.

Auditors used various methods to study the issues addressed in this report. These methods included reviewing applicable state laws, department policies and procedures, and information obtained from department staff; reviewing information on IT breaches and IT definitions; and interviewing and/or observing department officials and staff.[1]

In addition, auditors used the following specific methods to meet the audit objectives:

- To evaluate the security of the Department's information technology (IT) systems, auditors and an independent security consultant retained by the Office of the Auditor General tested applications and servers using both automated and more detailed security testing techniques. To identify the number and nature of the Department's IT systems, auditors interviewed staff, reviewed documents, and performed technical scanning techniques. Auditors identified over 600 critical IT systems. Using a risk-based approach, auditors then selected various IT systems to test with automated security scans. These scans identified potential vulnerabilities in the applications and associated servers. Based on the scan results, auditors selected IT systems for further detailed testing. This testing allowed auditors to identify the potential impact of these applications being compromised because of their vulnerabilities. Auditors also performed social engineering attacks, and reviewed access controls by testing user lists for terminated users, unused accounts, improper separation of rights, password expirations, and data access control lists. Because of the information's sensitive nature, specific information about the security weaknesses identified has been excluded from this report and shared only with appropriate department officials.

- To determine if the Department had an individual responsible for IT security with appropriate authority and if the Department had an adequate information security program, auditors analyzed the Department's IT security-related policies and other documents and compared them to state-wide requirements from the Arizona Department of Administration (ADOA), Arizona Strategic Enterprise Technology Office, and to IT standards and best practices.[2] Auditors also attended a meeting held by the Department's Information Security Steering Committee.

[1] IT definitions obtained from the following: Committee on National Security Systems. (2010). *National information assurance glossary*; and National Security Agency. (2012). *Securing data and handling spillage events*, Washington, DC.

[2] IT standards and best practice material reviewed included: (1) International Organization for Standardization. (2005). *Information Technology—Security techniques—Code of practice for information security management*, (2nd ed.). Geneva, Switzerland; (2) Ross, R., et al. (2012). *NIST Special Publication 800-30 Revision 1: Guide for conducting risk assessments*. Gaithersburg, MD: National Institute of Standards and Technology; and (3) Ross, R., et al. (2013). *NIST Special Publication 800-53 Revision 4: Security and privacy controls for federal information systems and organizations*. Gaithersburg, MD: National Institute of Standards and Technology.

- To assess the physical security of taxpayer information, auditors reviewed U.S. Internal Revenue Service (IRS) requirements for protecting taxpayer information; conducted observations of department staff in the Audit, Collections, Process Administration, and Taxpayer and External Services Divisions for compliance with various policies and procedures; and attempted to gain access to the Department's secure areas without proper security credentials.[1] Additionally, auditors interviewed staff at the ADOA and analyzed employee security badge access and employment status data provided by both the ADOA and the Department.

- Auditors' work on internal controls included reviewing and assessing department security policies and procedures, conducting observations of department staff; and performing the test work described in previous bullets. Auditors' conclusions on internal control are reported in Findings 1, 2, and 3 of the report.

[1] IRS requirements reviewed were in the following publication: United States Internal Revenue Service. (2014). *Publication 1075, Tax information security guidelines for federal, state, and local agencies*. Washington, DC.

AGENCY RESPONSE

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.

Performance Audit Division reports issued within the last 18 months

14-102	Gila County Transportation Excise Tax
14-103	Arizona State Board of Dental Examiners
14-104	Arizona Office of Administrative Hearings
14-105	Arizona Board of Executive Clemency
14-106	State of Arizona Naturopathic Physicians Medical Board
14-107	Arizona Department of Child Safety—Children Support Services—Emergency and Residential Placements
14-108	Arizona Department of Administration—Arizona State Purchasing Cooperative Program
15-101	Arizona Department of Child Safety—Child Abuse or Neglect Reports, Substantiation Rate, and Office of Child Welfare Investigations
15-102	Arizona Department of Administration—State-wide Procurement
15-103	Arizona Medical Board—Licensing and Registration Processes
15-104	Arizona Department of Transportation—Motor Vehicle Division
15-105	Arizona Department of Revenue—Use of Information Technology
15-CR1	Independent Review—Arizona's Child Safety System and the Arizona Department of Child Safety
15-CR1SUPP	Supplemental Report to the Independent Review—Arizona's Child Safety System and the Arizona Department of Child Safety
15-106	Arizona State Retirement System
15-CR2	Independent Operational Review of the Arizona State Retirement System's Investment Strategies, Alternative Asset Investment Procedures, and Fees Paid to External Investment Managers
15-107	Arizona Sports and Tourism Authority
15-108	Arizona Department of Administration—Personnel Reform Implementation
15-109	Arizona Department of Administration—Sunset Factors
15-110	Arizona Foster Care Review Board
15-111	Public Safety Personnel Retirement System
15-CR3	Independent Operational Review of the Public Safety Personnel Retirement System Investment Strategies, Alternative Asset Investment Procedures, and Fees Paid to External Investment Managers
15-112	Arizona Commerce Authority
15-113	Arizona Department of Transportation—Transportation Revenues
15-114	Arizona Department of Transportation—Sunset Factors
15-115	Arizona Radiation Regulatory Agency, Arizona Radiation Regulatory Hearing Board, and Medical Radiologic Technology Board of Examiners

Future Performance Audit Division reports

Arizona Department of Revenue—Sunset Factors

Arizona Department of Child Safety—Child Safety, Removal, and Risk Assessment Practices