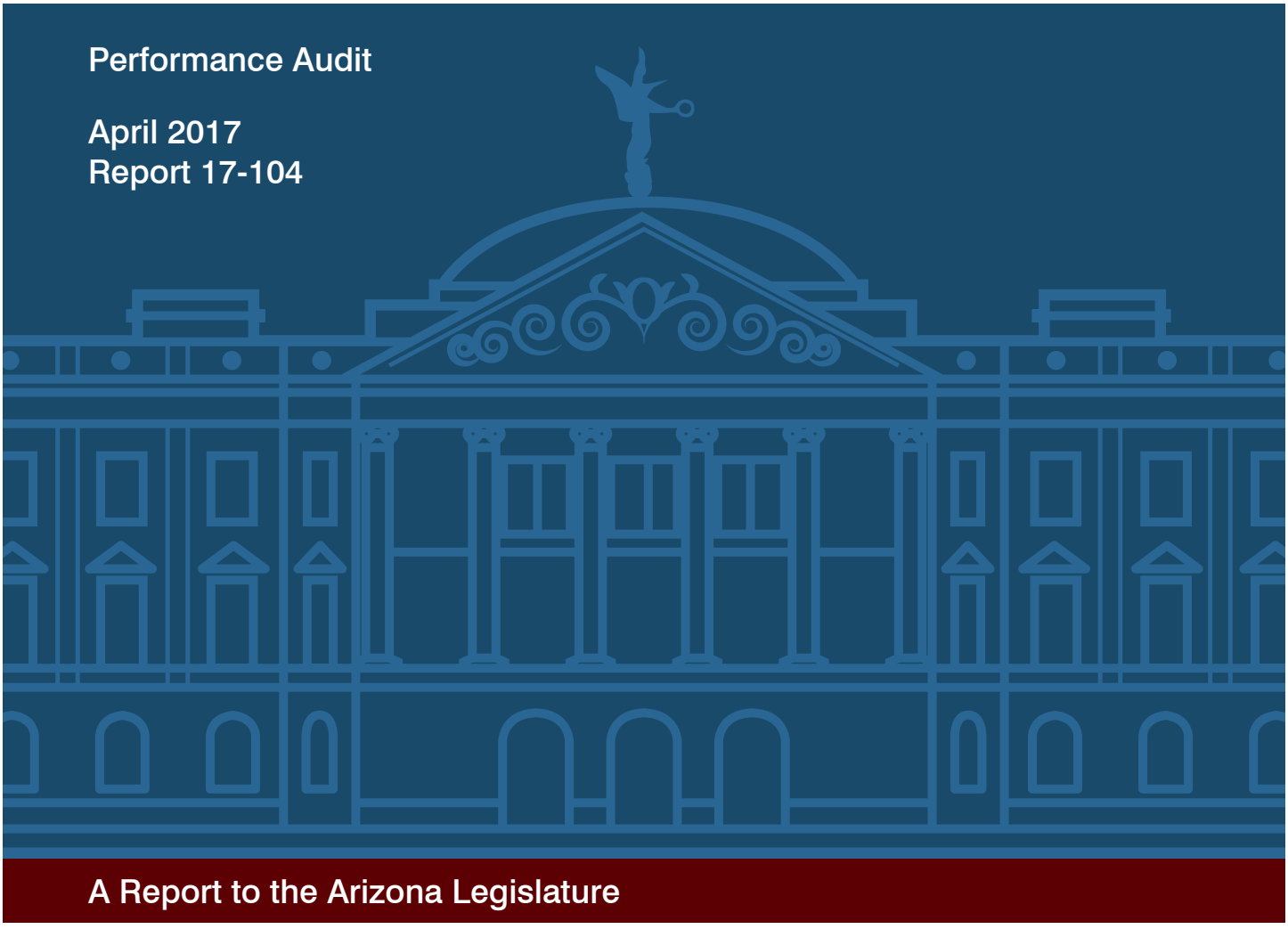
Arizona Department of Economic Security
Information Technology Security

Department should improve security processes and controls over its information technology systems and data, and establish an information security program



Performance Audit

April 2017
Report 17-104

A Report to the Arizona Legislature

Debra K. Davenport
Auditor General

ARIZONA Auditor General
Making a Positive Difference

ARIZONA Auditor General

Making a Positive Difference

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 and special reviews of school districts, state agencies, and the programs they administer.

The Joint Legislative Audit Committee

Senator **Bob Worsley**, Chair
Senator **Sean Bowie**
Senator **Judy Burges**
Senator **Lupe Contreras**
Senator **John Kavanagh**
Senator **Steve Yarbrough** (ex officio)

Representative **Anthony Kern**, Vice Chair
Representative **John Allen**
Representative **Rusty Bowers**
Representative **Rebecca Rios**
Representative **Athena Salman**
Representative **J.D. Mesnard** (ex officio)

Audit Staff

Dale Chapman, Director
Dot Reinhard, Manager and Contact Person
Melinda Gardner, Manager

Brian Miele, Team Leader
David Godfrey
Nicole Palmisano

Contact Information

Arizona Office of the Auditor General
2910 N. 44th St.
Ste. 410
Phoenix, AZ 85018

(602) 553-0333

www.azauditor.gov

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

April 18, 2017

Members of the Arizona Legislature

The Honorable Doug Ducey, Governor

Mr. Henry Darwin, Interim Director
Arizona Department of Economic Security

Transmitted herewith is a report of the Auditor General, *A Performance Audit of the Arizona Department of Economic Security (Department)—Information Technology Security*. This report is in response to an October 22, 2014, resolution of the Joint Legislative Audit Committee. The performance audit 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 Department 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


ARIZONA
Auditor General
Making a Positive Difference

ARIZONA Auditor General
Making a Positive Difference

REPORT HIGHLIGHTS
Performance Audit
April 2017

Arizona Department of Economic Security
Information Technology Security

CONCLUSION: The Arizona Department of Economic Security (Department) has a significant responsibility to safeguard its information technology (IT) systems and the data contained in them from misuse or attack because of the volume and nature of the sensitive data it maintains. Although the Department has established various IT security processes to help protect its IT systems and data, by performing common attack patterns, we identified weaknesses that allowed us access to these IT systems and sensitive data, including social security numbers and confidential health information. Additionally, the Department lacks an information security program as required by state policy. Establishing such a program would help ensure the Department sufficiently protects its IT systems and data. Finally, our in-depth review of three key policy areas—data classification, incident response, and security awareness education and training—found that the Department had not developed or fully developed associated procedures and had not incorporated some best practices within its incident response policy.

Department responsible for safeguarding its systems and data

As of December 2016, the Department reported using more than 120 IT systems or applications to store and process large volumes of sensitive data to administer various programs. These programs provide many services, such as unemployment insurance benefits, cash and/or nutrition assistance, child care assistance, and adult protective services, to assist more than 2 million Arizonans in need annually. Because of the volume and nature of the sensitive data the Department maintains—which includes names, social security numbers, driver license or state identification numbers, mailing addresses, and other information—it is a potential target for malicious attacks. The Department's responsibility to protect its data is specified in various federal and state laws and regulations, which include requirements for safeguarding health information and federal tax information.

Department should improve security processes and controls over its IT systems and data

Department's IT systems and sensitive data exposed because of security weaknesses—By simulating common attack patterns and exploiting security weaknesses, we accessed the Department's core IT systems and the sensitive data contained in them. Specifically, we exploited a weakness in the Department's network and gained unauthorized access to IT systems and sensitive data. With this access, we could control all network user accounts and view, alter, or delete confidential health information and other sensitive data. We also gained unauthorized access to sensitive data by exploiting security flaws in one of the Department's external web-based applications. Finally, we gained unauthorized access to IT systems and sensitive data through various social engineering techniques that requested department employees to perform actions and/or provide information needed to gain access.

Department has various IT security processes but should take steps to strengthen them—Although the Department has established various IT security processes and took steps to fix the specific security weaknesses we identified, its processes are not sufficiently robust to effectively identify, prevent, and remediate IT security weaknesses. Therefore, the Department needs to take several steps to more effectively secure its IT systems and the sensitive data contained in those systems. Specifically, the Department should improve three key security management processes: (1) vulnerability management, which involves systematically identifying, reviewing, and correcting IT system vulnerabilities; (2) patch management, which entails applying patches, or updates and fixes, to systems to ensure they remain secure; and (3) system configuration, which helps to ensure that the settings that control how systems operate are securely configured. In addition, the Department should strengthen its process for restricting access to its IT systems, including ensuring that user accounts for terminated employees are disabled or removed as soon after the employee leaves as is practical. Further, the Department should develop and implement a continuous process for monitoring system activity and policies, procedures, and practices for securely developing web-based applications.

Recommendations

The Department should develop or continue to develop and implement written policies and procedures for:

- Improving its vulnerability assessment, patch management, and system configuration processes;
- Ensuring the access-removal process is properly conducted;
- Establishing a continuous monitoring program for critical IT activities; and
- Developing, securing, and testing web-based applications.

Department should establish an information security program

Department has not established an information security program—To help ensure IT security state-wide, the Arizona Department of Administration, Arizona Strategic Enterprise Technology Office (ASET) requires state agencies to develop and implement an information security program. An information security program would help ensure that the Department has processes for identifying and safeguarding its IT systems and data against security vulnerabilities. Although the Department had developed a general policy outlining some requirements for an information security program, it lacked an overall security program that was consistent with ASET's requirements and best practices. For example, the Department had not conducted a department-wide IT risk assessment or developed procedures for doing so on a regular basis, and it had not adequately established the authority and responsibilities for information security.

Department should create written plan for developing an information security program—To help ensure the Department's IT systems and data are sufficiently protected, the Department should establish a written plan for developing and implementing a department-wide information security program. Consistent with ASET requirements, this plan should also address areas such as risk assessment; staff authority, roles, and responsibilities related to IT security; and the resources needed to implement an information security program.

Recommendations

The Department should:

- Establish a written plan for developing and implementing a department-wide information security program;
- Develop and implement department-wide IT risk assessment procedures;
- Further define information security program authority, roles, and responsibilities; and
- Ensure that needed resources are available to implement the program, such as staffing and budget.

Department should enhance efforts to establish information security policies and procedures

Department has not adequately implemented policies and procedures in three key information security areas—Although the Department has drafted or finalized policies for the 17 information security areas required by ASET, our review of three key areas—data classification, incident response, and information security awareness education and training—found that the Department had not incorporated some best practices within its incident response policy, and had not developed or improved the associated procedures to fully implement these policies.

Department had not implemented policies and procedures in other information security program areas—Our high-level review of several other ASET-required areas needed for a strong information security program found similar issues with inadequate, undeveloped, and/or unimplemented policies and procedures. For example, the Department's contingency planning policy, which states how it would restore unexpectedly unavailable data and operations, only applies to some systems and is missing critical best practices elements, such as detailed recovery procedures for restoring data. Further, the Department's written procedures for applying patches—or updates and fixes—to its IT systems inadequately address updating software and employee workstations. Without adequately developing policies and procedures to secure its IT systems and data, the Department is at a higher risk of a data breach.

Recommendations

The Department should:

- Further develop and implement information security policies and procedures for the areas of data classification, incident response, and information security awareness education and training; and
- Ensure its written plan for developing and implementing a department-wide information security program includes a process for adequately developing and implementing all ASET-required policies and procedures.

TABLE OF CONTENTS

INTRODUCTION

Scope and objectives

The Office of the Auditor General has conducted a performance audit of the Arizona Department of Economic Security (Department)—Information Technology (IT) Security pursuant to an October 22, 2014, resolution of the Joint Legislative Audit Committee. This audit is the third in a series of five audits conducted as part of the sunset review process prescribed in Arizona Revised Statutes (A.R.S.) 41-2951 et seq. It examines the effectiveness of department processes for safeguarding its IT systems and the data contained in them, including sensitive data. The first audit addressed the Department's processes for managing its Vocational Rehabilitation Services Program's rehabilitation service costs and clients' progress. The second audit addressed the Department's child care provider monitoring and complaint-handling processes. The two remaining audits will focus on the Department's licensing and oversight of homes for the developmentally disabled and the statutory sunset factors.

Department processes, uses, and stores large volumes of sensitive data

The Department provides a variety of services, such as unemployment insurance benefits, cash and/or nutrition assistance, child care assistance, and adult protective services, to assist more than 2 million Arizonans in need annually. To administer the department programs that provide these services, the Department uses many IT systems to store and process large volumes of sensitive data. For example, when applicants apply for unemployment insurance benefits through the Department's website, they must enter their name, social security number, driver license or state identification number, mailing address, and other information for the Department to process the application. Similarly, to apply for cash assistance, child care assistance, or nutrition assistance, applicants may need to provide names, social security numbers, birthdates, financial information, and health information. As of December 2016, the Department reported having more than 120 IT systems or applications.

Department responsible for safeguarding its systems and data

Because of the volume and nature of the sensitive data the Department maintains, it is a potential target for attacks by malicious individuals or organizations; therefore, the Department has a significant responsibility to safeguard its systems and data from misuse or attack. Various federal and state laws and regulations specify the Department's responsibility in protecting this data. For example, because the Department collects and uses both health information and federal tax information, the U.S. Department of Health and Human Services (HHS) and the Internal Revenue Service (IRS) have regulations that require the Department to protect its systems and this information. Specifically, HHS, under the Health Insurance Portability and Accountability Act (HIPAA), has established a set of security standards for protecting certain health information that is held or transferred in electronic form. These standards require that entities storing certain health information perform an ongoing risk analysis and implement policies and procedures that allow only authorized individuals to access health information and ensure that health information is not improperly altered or destroyed. In addition, the IRS has established specific requirements that the Department must follow regarding the use and protection of federal taxpayer information (FTI), including specific requirements pertaining to IT systems. For example, the IRS requires the Department to maintain an inventory of all department programs and systems that collect, use, maintain, and/or share FTI. Additionally, the IRS requires the Department to scan for vulnerabilities within its IT systems at least once a month. Arizona state agencies are also required to develop IT-security-specific policies and procedures consistent with a state-wide policy implemented by the Arizona Department of Administration, Arizona Strategic

Enterprise Technology Office (ASET) (see Finding 3, pages 21 through 25, for details about ASET-required policies). ASET's policies and procedures are intended to help state agencies implement recommended IT security best practices and to protect the State's IT infrastructure and the data contained in it.

Additionally, state law and federal regulations require agencies that collect, use, and store personally identifiable information—like the Department—to notify individuals affected by a breach—in other words, an incident in which sensitive data is inappropriately accessed, viewed, stolen, or stored. For example, A.R.S. §18-545 requires that any person or entity in Arizona holding electronic personal data notify all affected parties if it determines there has been a security breach in which unauthorized access to unredacted or unencrypted personal information has occurred.[1] Health-specific information is subject to a similar notification requirement under HIPAA. In addition to notifying the affected individuals, HIPAA also requires the organization that experienced the breach to notify the Secretary of HHS. Further, HIPAA requires that when an organization storing health information, like the Department, experiences a breach involving more than 500 residents of a state or jurisdiction, it must also notify prominent media outlets serving the area.

Proper IT security is vital to protecting the department systems that use and store sensitive data from security breaches. According to the Privacy Rights Clearinghouse, a nonprofit consumer education and advocacy organization dedicated to helping individuals protect their privacy, various government organizations reported approximately 79 electronic breaches affecting approximately 30 million people between 2012 and 2016 (see textbox, page 3, for examples of breaches).[2,3] Additionally, Symantec, a well-known IT security company, reported discovering more than 430 new pieces of malware in 2015, a 36 percent increase from the year before (see textbox).[4] Symantec estimated that security breaches resulted in more than half a billion lost or stolen records.

Malware—Malware is software intended to damage a computer, mobile device, or computer system, take control over its operation, or gather sensitive data. Malware can be used to facilitate a breach of an IT system.

Breaches have considerable costs to both organizations and individuals. For example, a research paper published in the *Journal of Cybersecurity* explained that the median loss from a data breach is $170,000.[5] Further, when the Utah Department of Health experienced a breach, the state spent $2.75 million in fiscal years 2012 and 2013 to address the breach (see textbox, page 3, for more information). Organizations that are breached must generally notify potential victims, may provide credit-monitoring services to victims, may experience legal and other costs, and may lose public trust. Further, individuals who have their information improperly accessed or stolen may spend time and resources monitoring their credit and may become victims of identity theft.

Department IT staff and expenses

The Department employs staff responsible for ensuring department IT systems and data are secure. The Department reported that, as of February 2017, its Division of Technology Services employed 259 staff. Of these staff, 32 were dedicated to IT security, including a Chief Information Security Officer (CISO), 4 employees who performed network security functions such as protecting the Department's email system, and others who

---

1 A.R.S. §18-545 does not apply to financial institutions obligated to protect nonpublic personal information of its customers per title V of the federal Gramm-Leach-Bliley Act, covered entities as defined under HIPAA, the Arizona Department of Public Safety, county sheriffs' departments, municipal police departments, prosecution agencies, or courts.

2 Privacy Rights Clearinghouse reported that this number fluctuates as new breaches are identified and reported. Likewise, breaches may be reported without information on the number of people affected.

3 This figure does not include breaches that occurred at educational institutions.

4 Symantec. (2016) *Internet Security Threat Report, Vol. 21*. Mountain View, CA.

5 Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 1-15. The median figure is calculated from a dataset of 602 data breaches, which the author defines as "the unintentional disclosure of personally identifiable information stemming from loss or theft of digital or printed information." Of the 602 data breaches, the losses ranged from near zero to $572 million.

Examples of electronic data breaches in government and healthcare

Banner Health—In August 2016, the Arizona hospital system Banner Health contacted 3.7 million individuals whose personal information may have been accessed because of a security breach in their system. Banner Health reported that the breach may have exposed credit card information and patient information such as names, birthdates, dates of service, claims information, and possibly health insurance and social security numbers. Additionally, information regarding health plans, beneficiaries, physicians, and healthcare providers may have been exposed. In response, Banner Health reported conducting an investigation, hiring a forensic firm, and providing a year of free credit monitoring to those whom the breach may have impacted.

U.S. Office of Personnel Management—In 2015, the U.S. Office of Personnel Management discovered that, through two separate but related security incidents, the background investigations and personnel records of current, former, and prospective federal employees and contractors had been compromised. In the first breach, the personnel data of 4.2 million former and current federal government employees was compromised. In the second breach, the background investigation records of approximately 21.5 million current, former, or prospective federal employees and contractors were compromised. The compromised information included social security numbers, address, date and place of birth, and other information. The federal government provided identity restoration service, identity theft insurance, and continuous identity and credit monitoring to those the breach impacted.

Anthem Healthcare—In 2015, 78 million patients had their personal information accessed through a data breach conducted by external hackers on Anthem Healthcare, a private company that provides health insurance. Personal identification information such as social security numbers, email addresses, and home addresses was accessed and compromised. Anthem Healthcare provided those affected with identity protection services.

Utah Department of Health—In March 2012, IT 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 the breach impacted. According to the Utah Department of Health, Utah spent $2.75 million in fiscal years 2012 and 2013 in response to the breach. In addition to the breach costs, Utah's governor requested a security review for all state agencies at a cost of $1.3 million.

Source: Auditor General staff analysis of information primarily from the websites of the organizations that were breached.

performed functions such as monitoring employee access to systems in various divisions.[6] Prior to November 2016, 21 of the 32 IT security staff were housed in various department divisions and reported to management in their respective divisions. However, in November 2016, the Department centralized its IT security functions by consolidating IT security employees from various divisions into a central management reporting structure under the CISO, as opposed to having security teams report to management in their respective divisions.

The Department estimated that it spent approximately $1.7 million in fiscal year 2016 for information security, including staff, equipment, and other expenses.

[6] The Department's other IT staff include systems project managers, programmer analysts, applications developers; and data center, service center, and help desk staff.

Department should improve security processes and controls over its IT systems and data

The Arizona Department of Economic Security (Department) should improve its information technology (IT) security processes and controls to ensure that its IT systems and the data contained within them, including sensitive data, are better protected from unauthorized access. Malicious attackers use various methods to try to exploit security weaknesses to gain access to and/or compromise IT systems, which may result in a disruption of services or the theft of sensitive data. Although the Department has established various IT security processes to help protect its IT systems and data, by performing common attack patterns, auditors discovered weaknesses that resulted in auditors gaining access to these IT systems and sensitive data, including social security numbers and confidential health information. To better protect its IT systems and the sensitive data contained in them, the Department should improve key security management processes, including its processes for identifying and correcting IT security vulnerabilities. In addition, the Department should enhance its processes for restricting access to and identifying and addressing unusual or unauthorized activity on its IT systems, and develop and implement written policies and procedures for developing, securing, and testing web-based applications.

Security attacks exploit IT weaknesses

Security weaknesses can be exploited to gain access to and/or compromise IT systems, which could result in a disruption of important services, or theft and/or loss of sensitive data (see Introduction, pages 1 through 3, for specific examples). 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, 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 of an entity's network—depending on the attacker, the attacker's 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 or over a long period of time during an attempt to gain access. Further, attackers may use social engineering in tandem with these steps to convince users to provide them with information or the means needed to obtain unauthorized access to IT systems (see textbox on page 6).

Social engineering—These 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:

- **Email phishing—**Sending devious emails 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.

Department's IT systems and sensitive data exposed because of security weaknesses

By simulating common attack patterns and exploiting security weaknesses, auditors accessed the Department's core IT systems and the sensitive data contained in them. Specifically, auditors exploited weaknesses in the Department's internal systems, an external web-based application, and its security awareness efforts. Specifically:

- **Internal systems security weakness allowed auditors to gain access to sensitive data—**As part of its IT security testing, auditors discovered and exploited a specific weakness in the Department's network and gained unauthorized access to IT systems and sensitive data.[7] Based on this access, auditors found that they could control all network user accounts, including accounts with high-level access. These accounts could then be used to view, alter, or delete confidential health information and other sensitive data, including client social security numbers, names, and addresses.

  Department staff reported that it began testing a fix for this specific issue in November 2016 shortly after auditors notified the Department of the security weakness, and the fix was implemented department-wide in January 2017. However, auditors also identified deficiencies in the Department's system configuration processes (see pages 9 through 10) that require the Department to take additional steps to adequately protect its systems and data. System configurations are settings that control how systems operate and should be designed in a secure manner whenever a new server, workstation, or other critical resource is introduced to the network environment.

- **Web application security flaws allowed auditors to gain access to sensitive data—**Auditors also gained unauthorized access to sensitive data by exploiting security flaws in one of the Department's external web applications (see textbox). Specifically, when auditors conducted manual testing on some of the Department's external web applications, auditors identified and exploited security weaknesses, which would have allowed them to view, alter, or delete sensitive data, including protected health information, names, and addresses for an estimated 100,000 individuals.

  A **web application** is a software program or system that is accessed by an end user to perform a transaction with a web browser, such as Internet Explorer, over a network such as the internet. An external web application is accessible from any user connected to the internet and could be more susceptible to attack.

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

  Auditors notified the Department of the discovered vulnerabilities, and the Department reported it fixed them in August 2016. However, the Department will need to take additional steps to ensure that all of its web-based applications are properly secured (see page 11 for more information).

- **Security awareness efforts did not prevent auditors from simulating successful social engineering attacks—**Finally, auditors gained unauthorized access to IT systems and data through security vulnerabilities

[7] Auditors were granted internal access to the Department's network to conduct automated testing on the Department's network and IT systems to attempt to identify security weaknesses and vulnerabilities.

identified during auditors' social engineering testing. For example, using various social engineering techniques that requested department employees to perform actions and/or provide information, auditors accessed the Department's internal network and could have accessed sensitive data within the Department's internal IT systems. Although some department controls intercepted or prevented some of auditors' social engineering attempts to access department systems and sensitive data, these controls did not successfully prevent all attempts. A substantial number of department staff were susceptible to the attacks, indicating potential deficiencies in the Department's security awareness user training and education programs. Specifically, auditors' phishing attack success rate on the Department was more than double the percentage of successful attacks outlined in a recent phishing susceptibility report where a similar attack method was used against government agencies.[8]

Auditors immediately notified the Department of the access they gained using social engineering techniques, and the Department reported that it was working on implementing several technical controls to correct the identified issues in addition to restructuring its annual security awareness training. Because various types of social engineering can be used, the Department should ensure that enhancements to its security awareness training and education program properly address all potential types of attacks. For example, using simulated social engineering exercises could help the Department identify and mitigate weaknesses within its security awareness training and education program (see Finding 3, pages 21 through 25, for recommendations to enhance the Department's security awareness training and education program).

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

Although the Department has established various IT security processes and took steps to fix the specific security weaknesses discovered by auditors, its processes are not sufficiently robust to effectively identify, prevent, and remediate IT security weaknesses. Therefore, the Department needs to take several steps to more effectively secure its IT systems and the data contained in those systems. Specifically, the Department should improve three key security management processes: (1) vulnerability management, which involves systematically identifying, reviewing, and correcting IT system vulnerabilities; (2) patch management, which entails applying patches, or updates and fixes, to systems to ensure they remain secure; and (3) system configuration, which helps to ensure that the settings that control how systems operate are securely configured. In addition, the Department should strengthen its process for restricting access to its systems, including ensuring that accounts for terminated employees are disabled or removed as soon after the employee leaves as is practical. Further, the Department should develop and implement a continuous process for monitoring system activity and policies, procedures, and practices for securely developing web-based applications.

Security management processes need improvement—Although the Department uses several IT security management processes, auditors identified three processes that need improvement to help better secure the Department's IT systems. Specifically:

- **Vulnerability management process should be developed and implemented—**Vulnerability management is the process of identifying vulnerabilities such as IT security weaknesses, evaluating the associated risks, and either correcting or mitigating the vulnerabilities or documenting the acceptance of the risks. Although the Department performs vulnerability scans of its IT systems, it has not created a documented vulnerability management process to help ensure this process is performed with sufficient rigor and timeliness. Specifically:
    - **Not all IT systems scanned for vulnerabilities—**Vulnerability scanning involves using automated tools to identify security weaknesses within networks and IT systems. The Department scans its IT systems on a regular, scheduled basis; however, the Department lacks a process to identify and inventory all IT systems and devices that should be scanned, such as servers, workstations, routers/switches, and applications. Therefore, although the Department reported that it scans most of its IT systems every

[8] PhishMe, Inc. (2015). *Enterprise phishing susceptibility report: An inside look at employee behavior pertaining to highly-effective phishing scenarios*. Leesburg, VA.

month, it cannot provide documentation to support that assertion. For example, auditors scanned 752 department servers in August 2016 and, after comparing auditors' results to the Department's scans, found that the Department had not scanned a majority of those servers that month.[9]

- **Vulnerability and penetration testing insufficient—**Vulnerability and penetration testing is the process of simulating attacks on IT systems by systematically looking for potential security weaknesses across the IT environment and then attempting to gain access to systems and data by exploiting these vulnerabilities. The Department does not routinely perform this type of testing but has hired contractors to perform these tests periodically. However, auditors identified several security issues using common attack methodologies that had not been previously discovered, highlighting shortcomings in the depth and frequency of the testing that is performed. In addition, department IT security staff do not have the knowledge or expertise required to identify common attack strategies currently used by hackers. For example, based on interviews with department staff, these staff were not adequately familiar with the strategies auditors used to attack the Department's IT systems.

- **Remediation process to address vulnerabilities lacking—**Remediation of identified vulnerabilities entails reviewing and addressing these vulnerabilities or formally accepting their associated risks, such as when business needs outweigh security requirements. However, the Department has not established an adequate remediation process. As a result, many identified vulnerabilities have not been addressed. For example, auditors scanned 752 department servers in August 2016 and found that more than 63 percent had critical and high vulnerabilities, some dating back to 1999. Department staff reported that historically, vulnerability reports were distributed to IT staff within each division who were directed to apply fixes. Additionally, due to varying remediation results, the Department moved this responsibility to two of its central IT security staff in February 2016, but because these staff have other job functions, auditors determined this to be an inadequate distribution of resources assigned to vulnerability management activities. The Department also reported that moving the IT staff distributed across the Department into its newly centralized IT security structure should help improve the efficiency of vulnerability management processes (see the Introduction, page 3, for more information on the centralization effort).

To help ensure vulnerabilities are effectively identified and addressed, the Department should develop and implement written policies and procedures establishing a formal vulnerability management process. Specifically, as part of its vulnerability management process, the Department should:

- Ensure that regular vulnerability scanning occurs and is comprehensive, meaning that it includes all systems. To do so, the Department will need to develop and implement procedures for identifying and creating an inventory of all systems, such as with automated tools or software.

- Include regular, comprehensive vulnerability and penetration testing. If the Department chooses to continue using contractors to perform this work, it should ensure its contractors effectively identify vulnerabilities by conducting more frequent, comprehensive testing. If the Department will primarily rely on using internal staff for vulnerability and penetration testing, the Department will need to develop in-house expertise on vulnerability and penetration testing, including common attack strategies currently used by hackers. For example, in addition to formal training, widely used IT security sources, such as IT security conferences and blogs, contain information on the newest attack methods and defenses.

- Include a well-defined remediation process. This process should identify the specific staff responsible for addressing identified vulnerabilities, including the number and type of staff involved; specify staff roles and responsibilities related to reviewing and addressing detected vulnerabilities or formally accepting their associated risks; and set specific time frames for completing the remediation process.

[9] Auditors found that the Department had not scanned 74 percent of the 752 servers auditors scanned. However, according to the Department, its August 2016 scan was the first one conducted after the Department moved its data center, and this move could have impacted the results of its scan.

- Train appropriate staff on the vulnerability management process and the supporting policies and procedures.

- **Patch-management process should be improved—**Patch management is another important process for helping to secure IT systems and data. Hardware and software vendors periodically issue updates, or patches, to their products to correct security vulnerabilities and additional flaws that have been identified, and to improve usability, performance, and security. 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 has begun to develop policies and procedures to guide its patch-management process and performs some patching on most of its IT systems, its process does not include some older systems and third-party software, which require updates to mitigate vulnerabilities. As a result, patching is performed inconsistently, and many of the Department's IT systems are not fully updated with necessary and recommended patches. Specifically, auditors discovered third-party software and operating system security updates that had been available for several years but had not been applied on 354 of the 752 department servers that auditors reviewed, or 47 percent, resulting in vulnerabilities that potentially place department systems and data at risk.

  To improve its patch management process, the Department should continue to develop and implement written patch management policies and procedures to guide its staff and efforts in this area. These written policies and procedures should include the following:

  - Identifying and determining the third-party software and operating system security updates that are available and whether a software or system update should be applied, including testing and documenting the effectiveness and potential side effects of available patches before installation;

  - Applying available patches in a timely manner and reviewing third-party software and operating system security updates to ensure they are effectively applied; and

  - Accepting, justifying, and documenting the risk of not updating the software or system if there are extenuating circumstances, such as older applications that may not be able to run or will not perform properly with the updates applied.

- **IT system configuration process should be strengthened—**The Department does not sufficiently review the configurations of its servers, workstations, and other critical network resources to ensure that they are as secure as possible. Configurations are settings that control how systems operate, such as software that is appropriate to install on a server versus a workstation and services that should or should not be run. IT servers and other devices, such as IT storage systems, provide and hold a significant portion of the critical functionality and sensitive data department employees need to complete their job duties. When IT systems are not properly configured, errors may occur, system functionality may be inhibited, and data contained within those systems may be more susceptible to attacks.

  Auditors' review determined that the Department has improper server configurations and unnecessary services and applications enabled on many of its IT systems, which unnecessarily expose these systems to risks. Specifically, auditors found that an unnecessary configuration was enabled on some of the Department's workstations, a configuration that allowed auditors to gain access to other resources within the Department's internal network and unauthorized access to sensitive data. Although a draft policy regarding system configuration had been created, auditors found that the Department had not performed some commonly recommended configuration changes that would have mitigated certain vulnerabilities and that cannot otherwise be resolved by installing a patch. In addition, the Department's process for configuring some of its IT resources contained common settings that, if not individualized or randomized, could provide potential attackers with a means to move from system to system. Some critical settings need to be made unique to limit the broad access that could otherwise result.

  To address these issues, the Department should continue its efforts to develop and implement written policies and procedures for securely configuring its IT systems. These policies and procedures should include requirements for:

- Configuring the Department's IT systems so that they do not provide more functionality than is necessary, including provisions and controls to ensure that baseline configurations, which provide an agreed-upon set of attributes that serve as a basis for information system settings, are developed and documented for each IT system, as appropriate;
- Developing and documenting specific configuration settings;
- Ensuring unique or randomized settings are used for critical functionality; and
- Defining the frequency of reviews and of updates to configurations.

Process for restricting access to only authorized users should be strengthened—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 data and related data-processing systems or services, or entering specific physical facilities. Although the Department has some controls in place, such as access forms and an electronic ticketing system to document access, auditors identified some deficiencies that provide excessive access to the Department's IT systems. Specifically:

- **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 the Department's network found numerous active accounts that were either unused or linked to terminated employees. In addition, access for the network 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 and the sensitive data they contain. To ensure the access-removal process is properly conducted, the Department should develop and implement written policies and procedures for reviewing and adjusting, as needed, user access and account access privileges periodically, and ensure that accounts for terminated or separated employees are disabled or removed as soon after the employee leaves as is practical.
- **Some passwords not changed frequently—**The Department has established a policy that requires passwords on all network accounts to be changed at least once every 30 days; however, auditors found numerous accounts with passwords that were older than 30 days. Many 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; yet, 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 had prior knowledge of these account passwords could still have access to them, and any malicious user who gains access to such credentials may have been able to obtain access to the corresponding systems. In addition, the Department has not established a process for evaluating the need to change these passwords based on the separation of individuals who had access to these passwords based on their 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 in accordance with its policies.

Continuous IT system log monitoring program should be developed and implemented—The Department has not adequately monitored the logs that capture information for its IT systems' user and computer activities. Collecting and monitoring logs of critical IT system activities enable organizations to track events on IT systems and networks and to detect improper actions by any person who may access its IT systems, 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. However, auditors found that the Department's monitoring activities were insufficient. For example, although the Department reported it detected auditors' testing of external web applications, it did not detect auditors' attempts and success in obtaining unauthorized access to the Department's internal network.

To improve its log-monitoring efforts, the Department should develop and implement a continuous log-monitoring program that includes written policies and procedures for monitoring critical IT activities. The Department's policies and procedures should:

- Describe the IT systems and functions within each IT system that should be logged;
- Specify how frequently each log should be monitored;
- Identify who is responsible for ensuring log events are captured and reviewing log events on a regular basis;
- Develop standard response actions that should be taken for detected events, including informing designated personnel of security risks to the Department and for individual information systems; and
- Include requirements for securely protecting the logs and time frames for how long the logs should be retained before being deleted.

Process needed to incorporate security when developing web-based applications—To better ensure the security of web-based applications, the Department should establish department-wide security standards for developing, securing, and testing web-based applications that are in line with IT standards and best practices. Although the Department develops new web-based applications using a department-wide standard, the standard lacks detailed security requirements and guidance for developers. As a result, the Department's web-based applications may be developed with security weaknesses, such as the weakness discovered by auditors in one of the Department's external web applications. In addition, the Department's web-based application development processes do not include comprehensive security testing requirements or processes. For example, auditors interviewed department staff and found that web applications are not evaluated for security vulnerabilities individually prior to being put into service.

According to IT standards and best practices, building security into the web-based application development process is more cost-effective and secure than applying it afterwards.[10,11] These IT standards and best practices also recommend that organizations' application development process employ security practices and requirements during all phases, including the definition of requirements, design and construction of the application, testing, and implementation. Therefore, the Department should develop and implement written policies and procedures for developing, securing, and testing web-based applications. The Department's policies and procedures should include the following:

- **Gathering security requirements—**Security requirements should include classifying the data in the application according to confidentiality and defining how the web-based application will comply with all relevant laws, regulations, and standards.
- **Up-to-date secure coding standards or conventions—**These are the steps that should be followed to develop a web-based application based on best practices.
- **Threat modeling during development—**Threat modeling involves defining how the application works, exploring potential vulnerabilities and threats by thinking of possible ways an attacker would attack the application, and then developing mitigating controls for each of the realistic threats identified.
- **Source code review—**Source code review is the process of manually checking the web-based application's operational structure for security issues that cannot be detected with any other form of analysis or testing.
- **Security testing before releasing a web-based application to the live environment—**Security testing before release helps ensure that the web-based application functions as intended and does not contain critical flaws when it is released.

[10] Open Web Application Security Project. (2014). *OWASP testing guide, version 4.0*. Bel Air, MD: OWASP Foundation.

[11] Open Web Application Security Project, 2014.

Recommendations

1.1. To help ensure vulnerabilities are effectively identified and addressed, the Department should develop and implement written policies and procedures establishing a formal vulnerability management process. Specifically, as part of its vulnerability management process, the Department should:

a. Ensure that regular vulnerability scanning occurs and is comprehensive, meaning that it includes all systems. To do so, the Department will need to develop and implement procedures for identifying and creating an inventory of all systems, such as with automated tools or software.

b. Include regular, comprehensive vulnerability and penetration testing. If the Department chooses to continue using contractors to perform this work, it should ensure its contractors effectively identify vulnerabilities by conducting more frequent, comprehensive testing. If the Department will primarily rely on using internal staff for vulnerability and penetration testing, the Department will need to develop in-house expertise on vulnerability and penetration testing, including common attack strategies currently used by hackers. For example, in addition to formal training, widely used IT security sources, such as IT security conferences and blogs, contain information on the newest attack methods and defenses.

c. Include a well-defined remediation process. This process should identify the specific staff responsible for addressing identified vulnerabilities, including the number and type of staff involved; specify staff roles and responsibilities related to reviewing and addressing detected vulnerabilities or formally accepting their associated risks; and set specific time frames for completing the remediation process.

d. Train appropriate staff on the vulnerability management process and the supporting policies and procedures.

1.2. The Department should continue to implement written patch management policies and procedures to guide its staff and efforts in this area. These written policies and procedures should include the following:

a. Identifying and determining the updates that are available and whether a software or system update should be applied, including testing and documenting the effectiveness and potential side effects of available patches before installation;

b. Applying available patches in a timely manner and reviewing the updates to ensure they are effectively applied; and

c. Accepting, justifying, and documenting the risk of not updating the software or system if there are extenuating circumstances, such as older applications that may not be able to run or will not perform properly with the updates applied.

1.3. The Department should continue its efforts to develop and implement written policies and procedures for securely configuring its IT systems. These policies and procedures should include requirements for:

a. Configuring the Department's IT systems so that they do not provide more functionality than is necessary, including provisions and controls to ensure that baseline configurations, which provide an agreed-upon set of attributes that serve as a basis for information system settings, are developed and documented for each IT system, as appropriate;

b. Developing and documenting specific configuration settings;

c. Ensuring unique or randomized settings are used for critical functionality; and

d. Defining the frequency of reviews and of updates to configurations.

1.4. To ensure the access-removal process is properly conducted, the Department should develop and implement written policies and procedures for:

a. Reviewing and adjusting, as needed, user access and account access privileges periodically, and ensure that accounts for terminated employees are disabled or removed as soon after the employee leaves as is practical.

b. Establishing requirements and time frames for changing service account passwords, and ensure that all passwords are changed in accordance with its policies.

1.5. The Department should develop and implement a continuous log-monitoring program that includes written policies and procedures for monitoring critical IT activities. The Department's policies and procedures should:

a. Describe the IT systems and functions within each IT system that should be logged;

b. Specify how frequently each log should be monitored;

c. Identify who is responsible for ensuring log events are captured and reviewing log events on a regular basis;

d. Develop standard response actions that should be taken for detected events, including informing designated personnel of security risks to the Department and for individual information systems; and

e. Include requirements for securely protecting the logs and time frames for how long the logs should be retained before being deleted.

1.6. The Department should develop and implement written policies and procedures for developing, securing, and testing web-based applications. The Department's policies and procedures should include the following:

a. Gathering security requirements;

b. Up-to-date secure coding standards or conventions;

c. Threat modeling during development;

d. Source code review; and

e. Security testing before releasing a web-based application to the live environment.

Department should establish an information security program

The Arizona Department of Economic Security (Department) should develop and implement an information security program. The Department lacks an information security program as required by state policy, and establishing such a program would help ensure that the Department sufficiently protects its information technology (IT) systems and the data contained in them, including sensitive data. Therefore, the Department should create a written plan to guide the development and implementation of a department-wide information security program. Consistent with state requirements, this plan should address areas such as risk assessment, staff roles and responsibilities, training, and resources related to its IT systems and data.

Department lacks information security program

The Department has not established an information security program as required by state policy. To help ensure IT security state-wide, the Arizona Department of Administration, Arizona Strategic Enterprise Technology Office (ASET) requires state agencies to develop and implement an information security program.[12] An information security program would help ensure that the Department has processes for identifying and safeguarding its IT systems and data against security vulnerabilities, such as those auditors identified (see Finding 1, pages 5 through 13). Although the Department had developed a general policy outlining some requirements for an information security program as of November 2016, it lacked an overall security program that was consistent with ASET's state-wide security program policy requirements and best practices. Specifically, the Department:

- **Has not conducted a department-wide IT risk assessment—**Although the Department approved a written risk assessment policy in September 2015, it has not conducted a department-wide IT risk assessment or established procedures for doing so. A risk assessment is a structured process that identifies risks within the organization, such as weak security practices, outdated systems, or the lack of a plan for restoring IT or other business operations following a disaster, and determines what controls are needed to lessen these risks. Risk assessments are also used to identify threats that originate outside of the Department, such as individuals attempting to disrupt or gain unauthorized access to the Department's IT systems, or fires and other unexpected events that could damage IT equipment. However, the Department has not performed a department-wide IT risk assessment or developed procedures for doing so on a regular basis. Instead, the Department primarily learns about security risks from external parties conducting periodic work with a limited scope, such as external auditors assessing only some portions of some IT systems and contractors using limited techniques to conduct vulnerability scans of only some portions of the Department's computer network. Without procedures for conducting a department-wide risk assessment, the Department cannot effectively identify potential IT security risks and then develop a plan for mitigating those risks.

- **Has not adequately established authority and responsibilities for an information security program—**IT standards and best practices indicate that to provide effective management, direction, and support for information security, an information security program should be formalized into a department-wide written plan that identifies a governance structure, or the method by which information security will be directed,

[12] Arizona Revised Statutes §18-105 requires the Arizona Department of Administration to develop and implement standards for state-wide information security and privacy.

administered, and/or controlled.[13] These standards and best practices also recommend that the plan should be disseminated and communicated to appropriate persons. Although the Department established a chief information security officer (CISO) position as early as 2006, it was not until September 2015 that the Department established in its information security program policy that one of the CISO's responsibilities is to coordinate, develop, implement, and maintain the department-wide information security program. However, the Department has not established in policy the CISO's authority to enforce the information security program or prescribed how the CISO's authority would be communicated to other staff. As a result, department staff might not be aware of the CISO's authority to implement and enforce information security policies department-wide. For example, auditors interviewed three department IT staff members in different divisions who are responsible for securing significant department IT systems. All three indicated that they were unfamiliar with information security policies created by the CISO's team that pertained to their specific responsibilities and indicated that they could not recall instances where the CISO had enforced information security policies.

Additionally, in contrast to ASET requirements, the Department's information security program policy does not describe the roles and responsibilities of any other staff who would be responsible for implementing the information security program. Without this information, department staff may not know how to best support the CISO and the Department in developing and implementing the information security program, and some program responsibilities may be discontinued or stalled when turnover occurs with IT security staff. For example, the Department reported it had setbacks in some areas after some IT security staff members, including staff responsible for developing IT policies and/or procedures, left the Department.

- **Has not developed and implemented information security procedures—**As part of an information security program, ASET has required state agencies to develop and implement policies and procedures in 17 security areas. These areas focus on processes such as data classification, security awareness education and training, and incident response, and are based on IT standards and best practices.[14] ASET required state agencies to have draft policies for the 17 areas established by July 2015 and has worked on additional policies that may be required in the future. As of November 2016, the Department had established or drafted the 17 required policies, but it had not yet developed or fully developed the associated procedures—the written steps the Department would take to implement these required policies—consistent with ASET requirements (see Finding 3, pages 21 through 25, for more information on some of these areas). The Department reported that staff turnover, including in the CISO position and other positions responsible for drafting IT policy, had hampered its efforts to develop the ASET-required policies and associated procedures. However, absent the ASET-required procedures, the Department cannot ensure that it is taking the necessary steps to effectively safeguard its IT systems and data, and its staff may not fully understand their responsibilities related to helping ensure IT security.

Department should create written plan for developing an information security program

To help ensure the Department's IT systems and data are sufficiently protected, the Department should establish a written plan for developing and implementing a department-wide information security program. The Department's plan should identify the specific tasks required to develop and implement an information security program, time frames for completion, and persons responsible for completing the specific tasks. Consistent with ASET requirements, this plan should also address areas such as risk assessment, staff roles and responsibilities related to IT security, training, and resources. Specifically, the Department's written plan should include the following:

- **Establishing a department-wide risk assessment process—**ASET requirements and IT standards and best practices state that organizations should have documented policies and procedures for regularly performing organization-wide IT risk assessments. For example, according to IT standards and best practices,

[13] National Institute of Standards and Technology (NIST). (2013). *Security and privacy controls for federal information systems and organizations*. Washington, DC: U.S. Department of Commerce.

[14] The security areas are based on IT standards and best practices, such as NIST, 2013.

the risk assessment process should consist of a structured methodology and its results used to make changes to the security program (see textbox). Conducting a department-wide risk assessment would help the Department identify and prioritize its information security program efforts. For example, once the Department has identified the IT system and data risks across the Department, it could determine which risks are the most serious and should be addressed first, such as excessive vulnerabilities within department systems or ineffective security awareness and training procedures (see Finding 1, pages 5 through 13, for information on security risks auditors identified). Therefore, the Department should develop and implement department-wide IT risk assessment procedures that are consistent with ASET requirements and best practices, regularly perform department-wide IT risk assessments, document the results and potential impacts of the identified risks, and use the risk assessment results to prioritize its information security program efforts and address identified risks.

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 operational/environmental threats;
- Documents results and potential impacts of risks;
- Uses results to make changes to the security program and addresses risks; and
- Reports results to top management.

Source: Auditor General staff analysis of IT standards and best practices: International Organization for Standardization (ISO). (2013). *Code of practice for information security controls*, ISO/IEC 27002. Geneva, Switzerland; and NIST, 2013.

- **Further defining information security program authority, roles, and responsibilities—**The Department should take additional steps to clarify the CISO's authority and the roles and responsibilities of other department staff for the information security program. In November 2016, the Department centralized its IT functions, including IT security. As part of this effort, the Department consolidated IT security employees from various divisions under a central management reporting structure under the CISO, thus increasing central IT security staff from 11 to 32 employees. Prior to the centralization, department IT security staff operated independently from one another while providing support to their respective divisions. The centralization effort may help the Department enforce consistent information security standards department-wide and help ensure security staff have clear responsibilities and adequate oversight.

  However, because its information security program policy does not clearly establish the CISO's authority to enforce an information security program nor does it describe the roles and responsibilities of any other staff who would participate in implementing the program, additional policy clarification is needed. ASET policy and IT standards and best practices indicate that authority, roles, and responsibilities should be clearly defined for each position involved in developing and implementing an information security program. Therefore, the Department should strengthen the CISO's authority to monitor and ensure compliance with the program by including this responsibility in its information security program policy. In addition, the Department should ensure the roles and responsibilities of any other IT security staff who will be involved in implementing the information security program are clearly defined in its information security program policy.

- **Establishing required security procedures—**As recommended in Finding 3 (see pages 21 through 25), the Department should ensure that its written plan for developing and implementing an information security program includes a process for adequately developing and implementing all ASET-required policies and procedures. These policies and procedures should include the policy area mentioned previously related to developing an information security program, the three key security areas auditors assessed in detail in Finding 3, the remaining 13 ASET-required areas, and any other areas ASET requires in the future.

- **Establishing a workforce development strategy—**The Department should follow best practices to establish an IT security workforce development strategy, which is a structured approach to further develop the core information security skills of department staff who work on the information security program. Although the Department provides some training for IT staff, the training does not include elements of best practices for workforce development, such as defining the knowledge and skill levels needed to perform

job duties, conducting role-based training programs, and defining standards for measuring and building individual qualifications for employees with IT security-related positions.[15] IT security workforce development programs are important so that staff have the necessary skills to implement and maintain an information security program.

- **Assessing information security resources—**To help ensure the information security program is maintained, the Department should assess its resources, such as staffing levels and the budget needed to implement the information security program, and ensure that resources are available as needed. For example, although the Department has processes to request monies for specific, large IT projects, the Department should ensure that its current resources are being used effectively and efficiently and should develop a process to ensure it will have sufficient resources to implement and operate the information security program. In addition, although department IT management reported measuring ratios of security staff to computers and to total department staff, the Department has not determined whether it needs to adjust its staffing based on these ratios. The Department should analyze the number and type of staffing needed to implement an information security program and ensure it has adequate staff, whether through reassigning staff, contracting for additional services, or other means. Without sufficient planning and analysis, the Department may be less able to acquire sufficient monies and staff for information security, and critical duties may not be assigned or performed.

Finally, the Department should ensure all department staff are aware of its information security program, including the CISO's authority for establishing and enforcing compliance with the program. Therefore, the Department should also establish a method for regularly communicating the authority, roles, and responsibilities for the information security program to department staff.

Recommendations

2.1. To help ensure the Department's IT systems and data are sufficiently protected, the Department should establish a written plan for developing and implementing a department-wide information security program. The Department's plan should establish the specific tasks required to develop and implement an information security program, time frames for completion, and persons responsible for completing the specific tasks.

2.2. The Department's written plan for developing and implementing a department-wide information security program should include the following tasks:

a. Developing and implementing department-wide IT risk assessment procedures that are consistent with ASET requirements and best practices, regularly perform department-wide IT risk assessments, document the results and potential impacts of the identified risks, and use the risk assessment results to prioritize its information security program efforts and address identified risks.

b. Further defining information security program authority, roles, and responsibilities, including strengthening the CISO's authority to monitor and ensure compliance with the program by including this responsibility in its information security program policy, and ensuring the roles and responsibilities of any other security staff who will be involved in implementing the information security program are clearly defined in its information security program policy.

c. Establishing an IT security workforce development strategy consistent with best practices, such as defining the knowledge and skill levels needed to perform job duties, conducting role-based training programs, and defining standards for measuring and building individual qualifications for employees with IT security-related positions.

d. Assessing its resources, such as staffing levels and the budget needed to implement the information security program, and ensuring that resources are available as needed. For example, the Department should ensure that its current resources are being used effectively and efficiently and should develop a process to ensure it will have sufficient resources to implement and run the information security

[15] NIST, 2013.

program. In addition, the Department should analyze the number and type of staffing needed to implement an information security program and ensure it has adequate staff, whether through reassigning staff, contracting for additional services, or other means.

e. Establishing a method for regularly communicating the authority, roles, and responsibilities for the information security program to department staff.

Department should enhance efforts to establish information security policies and procedures

As a part of developing its overall information security program (see Finding 2, pages 15 through 19), the Arizona Department of Economic Security (Department) should continue and enhance its efforts to establish information security policies and procedures. As of November 2016, the Department had drafted or finalized the 17 information security policies required by the Arizona Department of Administration, Arizona Strategic Enterprise Technology Office (ASET). However, auditors' in-depth review of three key policy areas—data classification, incident response, and security awareness education and training—found that the Department had not developed or fully developed the associated procedures and had not incorporated some best practices within its incident response policy. In addition, as mentioned in Finding 2, the Department is missing required elements in another key policy area related to developing an information security program. Further, auditors' high-level review of the Department's efforts to establish several of the remaining 13 ASET-required policies and associated procedures identified similar concerns. Therefore, the Department should ensure that it further develops and implements information security policies and procedures consistent with ASET requirements and best practices for the areas of data classification, incident response, and information security awareness education and training. In addition, in conjunction with creating a written plan for developing and implementing an information security program as recommended in Finding 2, the Department should include in its written plan a process to ensure all ASET-required policies and procedures are adequately developed and implemented.

Department has not adequately implemented policies and procedures in three key information security areas

Although the Department has drafted or finalized policies for the 17 ASET-required information technology (IT) security areas as of November 2016, auditors' review of three key areas—data classification, incident response, and information security awareness education and training—found that the Department had not incorporated some best practices within one of these policies, and had not developed or needed to improve the associated procedures to fully implement these policies.

Department should establish data classification process—The Department has developed a data classification policy but has not yet created adequate procedures to implement this policy. A data classification process identifies whether data is sensitive and stipulates how it should be protected based on the data's inherent level of risk, considering things such as whether the data is public or confidential, which would include health information, taxpayer information, or personally identifiable information. In April 2015, the Department approved a data classification policy consistent with ASET requirements. In addition, the Department has inventoried its IT systems, an important requirement for being able to properly identify and classify data, and classified data in those systems known to contain federal taxpayer information.

However, the Department has not created adequate procedures to implement its data classification policy. Specifically, the Department has not inventoried and classified all the data that it processes and stores, such as health information or personally identifiable information, nor has it developed procedures for how it would do this. By not classifying its data, the Department runs the risk that it or its employees may provide external entities with access to data or other information they do not need and/or should not have. IT standards and best practices incorporated into ASET requirements indicate that data classification should include an organization-

wide classification process (see textbox). Therefore, the Department should develop and implement procedures for its data classification process that are consistent with ASET requirements, such as protecting the data based on its level of risk; for example, whether the data is confidential; and developing a data classification inventory that is updated regularly.

Data classification process criteria

A documented organization-wide data classification process should be established that:

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

Source: Auditor General staff analysis of IT standards and best practices: International Organization for Standardization (ISO). (2013). *Code of practice for information security controls*, ISO/IEC 27002. Geneva, Switzerland.; and National Institute of Standards and Technology (NIST). (2013). *Security and privacy controls for federal information systems and organizations*. Washington, DC: U.S. Department of Commerce.

Department should develop and implement incident response process—The Department has developed an incident response policy consistent with ASET standards, but the policy lacks areas recommended by best practices, and the Department has not yet created all procedures necessary to implement this policy. Incident response is the process of detecting, reporting, and responding to information security incidents, such as a breach involving confidential data. 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. Additionally, Arizona Revised Statutes §18-545 requires that any person or entity in Arizona holding electronic personal data notify all affected parties if it determines there has been a security breach in which unauthorized access to unredacted or unencrypted personal information has occurred. In December 2014, the Department established a general incident-response-planning policy.

Although the Department has an incident-response-planning policy, it needs to enhance its policy to ensure it is consistent with best practices. Specifically, the policy lacks information regarding information spillage response, which is recommended by best practices. 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.[16] Additionally, best practices recommend a comprehensive incident response plan that provides staff with detailed guidance and procedures to follow in response to an incident, but the Department lacks such a plan. Further, the Department has not developed procedures for its incident-response-planning policy related to incident response training, testing, and monitoring. IT standards and best practices incorporated into ASET requirements recommend organizations have a standardized, organization-wide process that identifies roles and responsibilities for the incident response process and provides the responding individuals with the authority to make critical decisions (see textbox). Therefore, the Department should enhance its incident-response-planning policy to include an information spillage response, identify roles and responsibilities for the incident response process, and provide responding individuals with the authority to make critical decisions. In addition, the Department should develop and approve a comprehensive incident response plan and associated procedures related to incident response training, testing, and monitoring.

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, 2013; and NIST, 2013.

Department should improve security awareness program—The Department has implemented an information security awareness training policy consistent with ASET requirements, but its security awareness training and education program lacks two processes and has not been as effective as it should be. Information security

[16] National Security Agency. (2012). *Securing data and handling spillage events*. Washington, DC.

awareness education and training helps to ensure that an organization's employees understand the meaning of information security, risks associated with information security, the importance of complying with information security policies, and their responsibilities for information security. These education and training efforts are critical to help employees detect and avoid information security problems and incidents. IT standards and best practices incorporated into ASET requirements 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 IT systems (see textbox). The Department had a few elements of security awareness in a policy as early as 2005 and approved a policy in September 2015 consistent with ASET requirements. For example, consistent with the policy, the Department has a mandatory security awareness training and education program during employee orientation and includes an annual test on security awareness that all employees are required to take to retain network access.

Information security awareness education and training criteria

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

- Awareness or training activities for all individuals with access to the organization's information or IT 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 or not giving credentials out over the phone).

Source: Auditor General staff analysis of IT standards and best practices: ISO, 2013; and NIST, 2013.

Despite its efforts, the Department lacks two security training processes—role-based training and an insider threat program—and its security awareness efforts have not been as effective as they should be. 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 staff responsibilities and liabilities related to these threats, or ensure its staff are equipped to support the Department's security policy during their normal work. The Department indicated that it would implement training that is specifically geared toward an individual's role within the Department, as ASET requires, in 2018. However, the Department has not created an insider threat program as recommended in best practices, which would include training on recognizing and reporting potential indicators of insider threats, such as staff attempts to gain access to information not required for job performance and malicious activity by employees and/or persons claiming to be employees. In addition, weaknesses in the Department's current training efforts contributed to auditors' successful social engineering attacks, as reported in Finding 1 (see pages 6 through 7). One approach the Department could take to better evaluate the effectiveness of its training efforts would be to simulate social engineering attacks similar to those used by auditors as described in Finding 1 and provide additional training to individuals who do not appropriately respond to simulated attacks.

Therefore, the Department should improve its information security awareness training and education program and procedures to ensure that they are effective and consistent with ASET requirements and best practices, such as implementing role-based training based on users' job duties and training for employees to recognize and report malicious activities internal to the Department. This training should inform users about common methods used by attackers, such as phishing emails and practical examples of phishing attacks to foster a more security-focused culture within the Department. In addition, the Department should simulate attacks to test the training's effectiveness and provide additional training to individuals who do not appropriately respond to simulated attacks.

Department has not implemented policies and procedures in other information security areas

Similar to the three key areas mentioned previously, the Department also has not implemented policies or developed and implemented written procedures in other ASET-required areas needed for a strong information security program. Specifically, as described in Finding 2 (see pages 15 through 19), the Department has not

implemented its policy and has not developed and implemented written procedures for one of the foundational ASET-required policies—establishing an information security program. In addition, auditors conducted a high-level review of several other ASET-required areas and found similar issues with policies and procedures that were inadequate, undeveloped, and/or not implemented. For example, the Department's contingency planning policy, which states how it would restore data and operations when that data unexpectedly becomes unavailable, applies to only some systems and is missing critical elements recommended by best practices, such as detailed recovery procedures for restoring data. Further, the Department's written procedures for applying patches—or updates and fixes—to its IT systems do not adequately address updating software and employee workstations. Finding 1 (see pages 5 through 13) provides further information on the weaknesses auditors identified in the Department's patching and update processes. Therefore, without adequately developing and implementing policies and procedures to secure its IT systems and data, the Department is at a higher risk of a data breach.

As of November 2016, the Department had begun to improve its process to ensure that its information security policies and procedures were developed and conformed with ASET requirements, but these efforts should be enhanced. As indicated in Finding 2 (see pages 15 through 19), the Department reported that staff turnover, including in the CISO position and other positions responsible for drafting IT policy, had hampered its efforts to develop these policies and associated procedures. During the audit, the Department began consolidating and revising prior IT security policies to be aligned with ASET requirements by dedicating a full-time IT policy-writing staff position and involving other staff with reviewing these policies. However, the Department reported that some policies needed to be revised and it has not adequately defined and documented when it will complete each associated procedure or how it will ensure that the procedures will align with ASET requirements. Therefore, as the Department creates its written plan for developing and implementing an information security program (see Finding 2), it should ensure that its written plan includes a process for adequately developing and implementing all ASET-required policies and procedures. This process should include documenting time frames for completing key steps such as developing each written procedure and specifying persons responsible for completing specific tasks, such as developing the procedures, reviewing them to ensure consistency with ASET requirements and best practices, and approving the policies and procedures.

Recommendations

3.1. The Department should ensure that it further develops and implements information security policies and procedures consistent with ASET requirements for the areas of data classification, incident response, and information security awareness education and training. Specifically, the Department should:

a. Develop and implement procedures for its data classification process that are consistent with ASET requirements, such as protecting the data based on its level of risk; for example, whether the data is confidential; and developing a data classification inventory that is updated regularly;

b. Enhance its incident-response-planning policy to include an information spillage response, identify roles and responsibilities for the incident response process, and provide responding individuals with the authority to make critical decisions;

c. Develop and approve a comprehensive incident response plan and associated procedures related to incident response training, testing, and monitoring; and

d. Improve its information security awareness training and education program and procedures to ensure they are effective and consistent with ASET requirements and best practices, such as implementing role-based training based on users' job duties and training for employees to recognize and report malicious activities internal to the Department. This training should inform users about common methods used by attackers, such as phishing emails and practical examples of phishing attacks to foster a more security-focused culture within the Department. In addition, the Department should simulate attacks to test the training's effectiveness and provide additional training to individuals who do not appropriately respond to simulated attacks.

3.2. As the Department creates its written plan for developing and implementing an information security program (see Finding 2, pages 15 through 19), it should ensure that its written plan includes a process for adequately developing and implementing all ASET-required policies and procedures. This process should include documenting time frames for completing key steps such as developing each written procedure and specifying persons responsible for completing specific tasks, such as developing the procedures, reviewing them to ensure consistency with ASET requirements and best practices, and approving the policies and procedures.

Methodology

Auditors used various methods to study the issues addressed in this report. These methods included reviewing applicable federal and state laws, the Arizona Department of Economic Security's (Department) policies and procedures, and information obtained from department staff; reviewing information on information technology (IT) breaches and IT definitions; and interviewing department officials and staff.

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

- To evaluate the security of the Department's IT systems and data, auditors 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. According to the Department, it has over 120 IT systems and applications. Using a risk-based approach, auditors selected various IT systems to test with automated and manual methods. These methods identified potential vulnerabilities in the applications and associated servers, and auditors selected IT systems for further detailed testing. This testing allowed auditors to identify the potential risks that these applications might be compromised because of their vulnerabilities. Auditors also performed phishing attacks via email and telephone and reviewed access controls by testing user lists for terminated users, unused accounts, and password expirations. Additionally, auditors assessed the appropriateness of the Department's various security processes. 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 adequate information security program and related policies and procedures, 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, Arizona Strategic Enterprise Technology Office and to IT standards and best practices. Further, auditors reviewed several IT systems to determine the extent that IT security-related policies had been implemented, such as policies related to data classification, restoring data and operations when that data unexpectedly becomes unavailable, and applying patches—or updates and fixes—to its IT systems. Finally, auditors interviewed various staff in multiple divisions throughout the Department.

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

Auditors conducted this performance audit of the Department 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 their appreciation to the Department's interim director, management, and staff for their cooperation and assistance throughout the audit.

AGENCY RESPONSE

DEPARTMENT OF ECONOMIC SECURITY
Your Partner For A Stronger Arizona

Douglas A. Ducey
Governor

Henry Darwin
Interim Director

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

Dear Ms. Davenport:

The Arizona Department of Economic Security appreciates the opportunity to provide a response to the Information Technology Security Audit conducted by your office that was received on April 5, 2017. The Department is committed to continuous quality improvement, transparency, and accountability.

Attached is the Department's response to your findings and recommendations. We look forward to sharing our progress in implementing these recommendations.

Sincerely,

Henry Darwin
Interim Director

Enclosure: ADES Information Technology Security Audit Response

Finding 1: Department should improve security processes and controls over its IT systems and data

Recommendation 1.1: To help ensure vulnerabilities are effectively identified and addressed, the Department should develop and implement written policies and procedures establishing a formal vulnerability management process. Specifically, as part of its vulnerability management process, the Department should:

Recommendation 1.1a: Ensure that regular vulnerability scanning occurs and is comprehensive, meaning that it includes all systems. To do so, the Department will need to develop and implement procedures for identifying and creating an inventory of all systems, such as with automated tools or software.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The department has implemented a process to inventory all assets in the environment consolidating data from all available collectors. This dynamic list is maintained continuously and forms the basis for server vulnerability scanning. It currently reflects 1181 servers (including DCS) in the environment. Servers are scanned every 10 to 14 days. While this process has been improved since auditor's test work, it is also worth noting that the August 2016 comparison used the first scanning inventory conducted after DES' data center move. IP address changes caused by that move made that scan particularly unreliable.

Recommendation 1.1b: Include regular, comprehensive vulnerability and penetration testing. If the Department chooses to continue using contractors to perform this work, it should ensure its contractors effectively identify vulnerabilities by conducting more frequent, comprehensive testing. If the Department will primarily rely on using internal staff for vulnerability and penetration testing, the Department will need to develop in-house expertise on vulnerability and penetration testing, including common attack strategies currently used by hackers. For example, in addition to formal training, widely used IT security sources, such as IT security conferences and blogs, contain information on the newest attack methods and defenses.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: Last year, the agency budgeted for penetration testing and application vulnerability scanning by a contractor on eight public-facing servers. The agency has recently scheduled penetration testing and vulnerability scanning by a contractor of all 75 public-facing applications and for 500 internal servers. In addition to extending this contract to all servers, the department has purchased application-scanning software and deployed it to security staff who will regularly run vulnerability scans on applications. Scans will be scheduled for existing applications and will be applied to all new applications before they are authorized for production. Licenses are provided to application developers to conduct scans during the development process.

Recommendation 1.1c: Include a well-defined remediation process. This process should identify the specific staff responsible for addressing identified vulnerabilities, including the

number and type of staff involved; specify staff roles and responsibilities related to reviewing and addressing detected vulnerabilities or formally accepting their associated risks; and set specific time frames for completing the remediation process.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Information Security Program Plan and the Incident Response Plan are scheduled for publication in May 2017. The process of vulnerability response and remediation will be well defined, as will the roles for each participant in the remediation process. Service level expectations are included. Recognizing that not every vulnerability can be immediately addressed, the procedures define a process for assessing risk, implementing compensating controls, and formally accepting risk. Accepted risks will be prioritized and cataloged and a formal program of mitigation planning, implementation, and progress monitoring will be documented and integrated with the enterprise risk management strategy.

Recommendation 1.1d: Train appropriate staff on the vulnerability management process and the supporting policies and procedures.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The agency will incorporate the vulnerability management program training requirements into the existing security awareness program and the role-based security courses that are currently being designed. Training will alert system users to the concept of vulnerability recognition and give them clear guidance on how to report vulnerabilities to a central point for analysis. Personnel with relevant roles in the incident response program will receive role-based training on vulnerability discovery integration, categorization and assessment of vulnerabilities; remediation or integration into the risk management process; and evaluation for configuration, training, or procedure changes.

Recommendation 1.2: The Department should continue to implement written patch management policies and procedures to guide its staff and efforts in this area. These written policies and procedures should include the following:

Recommendation 1.2a: Identifying and determining the updates that are available and whether a software or system update should be applied, including testing and documenting the effectiveness and potential side effects of available patches before installation;

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: This procedure is in place and will be defined in the Configuration Planning Procedure scheduled for publication in April 2017. Additionally, the agency has already put metric collection systems in place that will extract information from the two major automated patching systems to make real time metrics of patch management penetration levels and effectiveness visible to security engineers. Server patching is a formal part of the division's change management process. As such extensive testing, communication, and after-action review are conducted.

Recommendation 1.2b: Applying available patches in a timely manner and reviewing the updates to ensure they are effectively applied; and

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Configuration Planning Procedure defines a process for reviewing patches published by vendors and prioritizing them for deployment. To reduce the lag between vendor publication and patch application the Department has added 2 FTEs to this team and will maintain better system inventories, standardized configurations, and published maintenance schedules for network devices and is automating the patch process when possible. The metric collection process that is currently being implemented will provide data that will allow the agency to measure progress on efforts to reduce the average time between patch publication and patch application.

Recommendation 1.2c: Accepting, justifying, and documenting the risk of not updating the software or system if there are extenuating circumstances, such as older applications that may not be able to run or will not perform properly with the updates applied.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: As discussed above, the agency will include un-remediated vulnerabilities in the enterprise risk management framework. This will include identification of systems that cannot be immediately remediated without affecting business operations, examining applicable threats that might exploit those vulnerabilities, quantifying the risk associated with the threat/vulnerability combination, considering compensating controls, formally accepting risk, and documenting the long-term risk treatment plan for the system.

Recommendation 1.3: The Department should continue its efforts to develop and implement written policies and procedures for securely configuring its IT systems. These policies and procedures should include requirements for:

Recommendation 1.3a: Configuring the Department's IT systems so that they do not provide more functionality than is necessary, including provisions and controls to ensure that baseline configurations, which provide an agreed-upon set of attributes that serve as a basis for information system settings, are developed and documented for each IT system, as appropriate;

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The System Security Maintenance procedure, 1-38-8220, which is scheduled for publication in April 2017, has appendices that define baseline security configurations for each operating system within the agency's environment, the mainframe computer, and DES managed network devices. Those configurations are derived from recommended configurations engineered by the Center for Internet Security (CIS). These baseline configurations are designed to comply with FISMA, PCI, and

HIPAA configuration recommendations while providing all necessary functionality to users.

Recommendation 1.3b: Developing and documenting specific configuration settings;

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: As explained above, the agency is adopting baseline configurations for each operating system in the environment. Where the agency deviates from CIS baselines for operational reasons, the security control is evaluated in the context of other security controls in the environment, and becomes a part of the operating system specific appendix in the System Security Maintenance procedure, 1-38-8220.

Recommendation 1.3c: Ensuring unique or randomized settings are used for critical functionality; and

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The agency understands the Auditor General's concern with non-randomized configurations. The department will implement a solution within the next two months to address the issue. The department's long-term solution for this issue is an enterprise identity and management application, which it is pursuing during fiscal year 2018.

Recommendation 1.3d: Defining the frequency of reviews and of updates to configurations.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The frequency of reviews is defined in the Configuration Management Procedure scheduled for publication in April 2017.

Recommendation 1.4: To ensure the access-removal process is properly conducted, the Department should develop and implement written policies and procedures for:

Recommendation 1.4a: Reviewing and adjusting, as needed, user access and account access privileges periodically, and ensure that accounts for terminated employees are disabled or removed as soon after the employee leaves as is practical.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Account Management Procedure scheduled for publication in May 2017, defines a process for ensuring that accounts for terminated employees are deleted in a timely manner. The department is synchronizing data with ADOA HRIS and Active Directory to flag accounts for examination and has automated the suspension of inactive accounts. The department has just finished a review of the highest-level privileged accounts resulting in an 80% reduction by the end of March 2017.

Recommendation 1.4b: Establishing requirements and time frames for changing service account passwords, and ensure that all passwords are changed in accordance with its policies.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The agency has implemented a system that changes and randomizes service account passwords. This is documented in the Account Management Procedure, which will be published in May 2017.

Recommendation 1.5: The Department should develop and implement a continuous log-monitoring program that includes written policies and procedures for monitoring critical IT activities. The Department's policies and procedures should:

Recommendation 1.5a: Describe the IT systems and functions within each IT system that should be logged;

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The agency has engaged a vendor, Dell SecureWorks for log monitoring. Security staff will continue to monitor logs as well. These new processes are defined in the Security Audit Procedure due for publication in May 2017. The procedure also defines the process for long-term log retention including retention schedules.

Recommendation 1.5b: Specify how frequently each log should be monitored;

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: Please refer to the response explanation for recommendation 1.5a.

Recommendation 1.5c: Identify who is responsible for ensuring log events are captured and reviewing log events on a regular basis;

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Security Audit Procedure, scheduled for publication, in May 2017, will enumerate in an appendix all required logs, their retention period, the required review frequency, and the individuals responsible for each review.

Recommendation 1.5d: Develop standard response actions that should be taken for detected events, including informing designated personnel of security risks to the Department and for individual information systems; and

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Incident Response Procedure, due for publication in May 2017, will define the process for responding to incidents discovered while reviewing security or application logs.

Recommendation 1.5e: Include requirements for securely protecting the logs and time frames for how long the logs should be retained before being deleted.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: Please refer to the response explanation for recommendation 1.5a.

Recommendation 1.6: The Department should develop and implement written policies and procedures for developing, securing, and testing web-based applications. The Department's policies and procedures should include the following:

Recommendation 1.6a: Gathering security requirements;

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Systems Acquisition and Development procedure, due for publication in June 2017, defines the process for system acceptance including the manner in which security is applied to the development and testing phases of application development or acquisition.

Recommendation 1.6b: Up-to-date secure coding standards or conventions;

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Systems Acquisition and Development procedure will require the use of secure coding standards consistent with current security standards.

Recommendation 1.6c: Threat modeling during development;

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Systems Acquisition and Development procedure defines a three-step methodology for threat modeling during the development process consistent with current security standards.

Recommendation 1.6d: Source code review; and

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The System Security Acquisition and Development Procedure will require that individuals who have *secure coding* training approve source code prior to a system receiving authorization as a production release.

Recommendation 1.6e: Security testing before releasing a web-based application to the live environment.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The System Security Acquisition and Development Procedure defines the process for security testing prior do deploying an application.

Finding 2: Department should establish an information security program

Recommendation 2.1: To help ensure the Department's IT systems and data are sufficiently protected, the Department should establish a written plan for developing and implementing a department-wide information security program. The Department's plan should establish the specific tasks required to develop and implement an information security program, time frames for completion, and persons responsible for completing the specific tasks.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The agency has finalized its Information Security Program Policy and is drafting its Information Security Program Plan, which is due for publication in April 2017. The plan will define the information security program including roles, responsibilities, and schedules.

Recommendation 2.2: The Department's written plan for developing and implementing a department-wide information security program should include the following tasks:

Recommendation 2.2a: Developing and implementing department-wide IT risk assessment procedures that are consistent with ASET requirements and best practices, regularly perform department-wide IT risk assessments, document the results and potential impacts of the identified risks, and use the risk assessment results to prioritize its information security program efforts and address identified risks.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The agency has published its Risk Assessment Policy and is in the process of revising the Risk Assessment Procedure to conform to ASET standards. It is scheduled for publication in May 2017.

Recommendation 2.2b: Further defining information security program authority, roles, and responsibilities, including strengthening the CISO's authority to monitor and ensure compliance with the program by including this responsibility in its information security program policy, and ensuring the roles and responsibilities of any other security staff who will be

involved in implementing the information security program are clearly defined in its information security program policy.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Information Security Program Plan will fully define the role of the Chief Information Security Officer as well as other critical security staff clearly enumerating their responsibilities and the scope and authority of their positions.

Recommendation 2.2c: Establishing an IT security workforce development strategy consistent with best practices, such as defining the knowledge and skill levels needed to perform job duties, conducting role-based training programs, and defining standards for measuring and building individual qualifications for employees with IT security-related positions.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: Both the Information Security Program Plan and the Security Awareness Training and Education Procedure will provide explicit guidance for the desired qualifications of key positions within the Information Risk Management program. The plan will describe role-based training for those positions as well as defining a strategy for maintaining currency in the information security specialty required for their position. In addition, the Department is working with vendors to obtain qualified contractors to address vacancies due to turnover.

Recommendation 2.2d: Assessing its resources, such as staffing levels and the budget needed to implement the information security program, and ensuring that resources are available as needed. For example, the Department should ensure that its current resources are being used effectively and efficiently and should develop a process to ensure it will have sufficient resources to implement and run the information security program. In addition, the Department should analyze the number and type of staffing needed to implement an information security program and ensure it has adequate staff, whether through reassigning staff, contracting for additional services, or other means.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The agency will engage the service of an independent technology research firm to evaluate the staffing of various information security functions. This review has begun and will continue into the coming fiscal year.

Recommendation 2.2e: Establishing a method for regularly communicating the authority, roles, and responsibilities for the information security program to department staff.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The agency will include this regular communication as a part of the new Security Awareness Program scheduled to begin January 2018. In the

meantime, the agency will continue its program of regular emails to systems users regarding their role in the information security process.

Finding 3: Department should enhance efforts to establish information security policies and procedures

Recommendation 3.1: The Department should ensure that it further develops and implements information security policies and procedures consistent with ASET requirements for the areas of data classification, incident response, and information security awareness education and training. Specifically, the Department should:

Recommendation 3.1a: Develop and implement procedures for its data classification process that are consistent with ASET requirements, such as protecting the data based on its level of risk; for example, whether the data is confidential; and developing a data classification inventory that is updated regularly;

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Data Classification Procedure, scheduled for publication in April 2017, defines the process for system owners to classify the level of sensitivity in their systems. This process will be monitored by security staff for compliance and inclusion in the agency data inventory.

Recommendation 3.1b: Enhance its incident-response-planning policy to include an information spillage response, identify roles and responsibilities for the incident response process, and provide responding individuals with the authority to make critical decisions;

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Incident Response Procedure and the Privacy Procedure, due for publication in May 2017, define the process, roles, and communications responsibilities during an information spillage incident.

Recommendation 3.1c: Develop and approve a comprehensive incident response plan and associated procedures related to incident response training, testing, and monitoring; and

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The agency published an Incident Response Policy in November 2016, and the Incident Response Procedure is due for publication in May 2017. The procedure is comprehensive and will define processes for training, testing, and monitoring the program.

Recommendation 3.1d: Improve its information security awareness training and education program and procedures to ensure they are effective and consistent with ASET requirements and best practices, such as implementing role-based training based on users' job duties and training for employees to recognize and report malicious activities internal to the Department.

This training should inform users about common methods used by attackers, such as phishing emails and practical examples of phishing attacks to foster a more security-focused culture within the Department. In addition, the Department should simulate attacks to test the training's effectiveness and provide additional training to individuals who do not appropriately respond to simulated attacks.

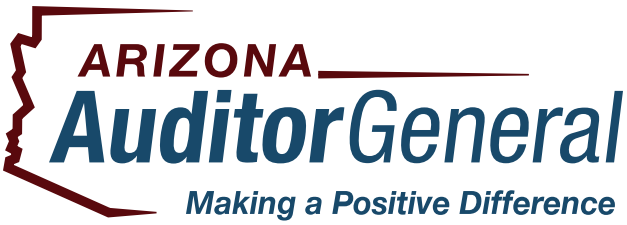
Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The agency will publish its Security Awareness Training procedure June 2017. This procedure will define the general awareness and role based training to be deployed to system users. It will emphasize awareness and extend the training using innovative methods to include each user in the information security effort. The agency will implement drills and simulated attacks to reinforce training.

Recommendation 3.2: As the Department creates its written plan for developing and implementing an information security program (see Finding 2, pages 15 through 19), it should ensure that its written plan includes a process for adequately developing and implementing all ASET-required policies and procedures. This process should include documenting time frames for completing key steps such as developing each written procedure and specifying persons responsible for completing specific tasks, such as developing the procedures, reviewing them to ensure consistency with ASET requirements and best practices, and approving the policies and procedures.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The agency has published all 17 of ASET's required security policies. Sixteen security procedures are in various stages of draft and are expected to be published between April and June 2017. The agency has a written schedule for publication of procedures including timeframes and responsible drafters, technical reviewers, and approval authorities.


ARIZONA
Auditor General
Making a Positive Difference