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.