STATE OF CONNECTICUT

AUDITORS' REPORT
DEPARTMENT OF ADMINISTRATIVE SERVICES
ELICENSE SYSTEM
INFORMATION TECHNOLOGY SECURITY AUDIT
AS OF JANUARY 2016

AUDITORS OF PUBLIC ACCOUNTS
JOHN C. GERAGOSIAN ❖ ROBERT M. WARD

Table of Contents

STATE OF CONNECTICUT

AUDITORS OF PUBLIC ACCOUNTS

State Capitol
210 Capitol Avenue
Hartford, Connecticut 06106-1559

JOHN C. GERAGOSIAN

ROBERT M. WARD

August 31, 2016

AUDITORS' REPORT
DEPARTMENT OF ADMINISTRATIVE SERVICES
ELICENSE SYSTEM
INFORMATION TECHNOLOGY SECURITY AUDIT
AS OF JANUARY 2016

We have audited certain operations of the Department of Administrative Services (DAS) eLicense System in fulfillment of our duties under Section 2-90 of the Connecticut General Statutes. The scope of our audit included, but was not necessarily limited to, the period ending January 2016. The objectives of our audit were to:

1. Evaluate the department's internal controls over significant management and financial functions;

2. Evaluate the department's compliance with policies and procedures internal to the department or promulgated by other state agencies, as well as certain legal provisions; and

3. Evaluate the economy and efficiency of certain management practices and operations, including certain financial transactions.

Our methodology included reviewing written policies and procedures, financial records, minutes of meetings, and other pertinent documents; interviewing various personnel of the department, as well as certain external parties; and testing selected transactions. We obtained an understanding of internal controls that we deemed significant within the context of the audit objectives and assessed whether such controls have been properly designed and placed in operation. We tested certain of those controls to obtain evidence regarding the effectiveness of their design and operation. We also obtained an understanding of legal provisions that are significant within the context of the audit objectives, and we assessed the risk that illegal acts, including fraud, and violations of contracts, grant agreements, or other legal provisions could occur. Based on that risk assessment, we designed and performed procedures to provide reasonable assurance of detecting instances of noncompliance significant to those provisions.

We conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards,* issued by the Comptroller General of the United States. Those standards require that we plan and perform our 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 such a basis.

The State Auditors' Findings and Recommendations in the accompanying report presents any findings arising from our audit of the Department of Administrative Services eLicense System.

COMMENTS

FOREWORD

The Department of Administrative Services operates primarily under the provisions of Title 4a, Chapter 57 of the Connecticut General Statutes.

A significant agency reorganization took place with the enactment of Public Act 11-51, effective July 1, 2011. The act absorbed the functions of certain other agencies into DAS. The former Department of Information Technology became the Bureau of Enterprise Systems and Technology (BEST) under DAS.

Section 4a-1 of the General Statutes provides that the department head shall be the Commissioner of Administrative Services, who shall be appointed by the Governor. Melody A. Currey was appointed commissioner, effective January 7, 2015, and served in that position throughout the audited period.

The Department of Administrative Services, Bureau of Enterprise Systems and Technology, administers the eLicense system, which can be accessed on the State of Connecticut eLicensing website. The system allows individuals and business entities to apply for various licenses, permits and registrations, which are administered by the Department of Public Health, Department of Consumer Protection, Department of Agriculture, State Board of Accountancy and the Office of Early Childhood. The system also allows individuals to verify a license, generate a roster, and download a roster.

STATE AUDITORS' FINDINGS AND RECOMMENDATIONS

Our review of the controls environment of the Department of Administrative Services Bureau of Enterprise Systems and Technology eLicense System revealed certain areas warranting attention that are discussed in the following findings.

Authentication Controls

Background: Most modern information systems do not store plaintext user passwords. Instead, they hash the passwords chosen by users, and store the hashes rather than the passwords. When a user logs in by entering a username and password, the password is hashed using the same algorithm originally used to hash it. If that hash matches the hash stored for the user, the login is successful. This creates a situation in which, were the database to be compromised, depending on the complexity of each user's password, it would take considerable time and/or be impossible to determine the user password, thereby limiting the security impact if they use the same password on other systems.

Hashing algorithms do not encrypt data, although it is often confused with encryption. A variable number of characters will always be hashed into the same number of characters if the same algorithm is used. In other words, a ten character password would have the same hash as a one thousand page novel, often 64 characters or less, depending on the hashing algorithm that is used. One cannot "decrypt" just 64 characters into the original thousand page novel. Hashing is not encryption and does not serve that purpose. It can, however, be used to determine whether something is the same as something else, and this is particularly useful for the storing of passwords, in which the text represented by a password is not important; all that is important is whether the text supplied by a user is or is not a match to the user's password.

Although storing hashed passwords is much safer than storing plaintext passwords, if user passwords are extremely simple, short in length, single words in the English dictionary, or the same as others commonly used, then they are prone to dictionary attacks. The hashes associated with many commonly used passwords are actually stored in lists that anyone can look up online with simple Google searches. This is one of the reasons why most systems have password length and complexity requirements in place. Even when the hashes are unknown and have not been compromised, such passwords would be easily guessable.

Criteria: The National Institute of Standards and Technology (NIST) recommends various identification and authentication controls (IA) in

its special publication 800-53 (SP 800-53). Control IA-5, Authenticator Management, requires the organization to:

a) Enforce minimum password complexity, including requirements for case sensitivity; number of characters; mix of upper-case letters, lower-case letters, numbers, and special characters; and include minimum requirements for each criteria;

b) Enforce a minimum number of changed characters when new passwords are created;

c) Enforce password minimum and maximum lifetime restrictions;

d) Prohibit password reuse for a defined number of generations.

Condition: eLicense password controls are currently configured in such a way that:

a) There are no length or complexity requirements;

b) Initial passwords set at user account creation do not have to be changed by the user at first login, so employees may use that default password indefinitely;

c) Passwords never expire, users can keep the same password indefinitely;

d) Passwords can be created that are identical to the associated username.

Items (b) and (c) above can be addressed by the user agencies in the configuration of their organization settings in eLicense. Items (a) and (d) are not currently configurable by the agencies.

At the time of our testing, there were 17 passwords used by two or more users of eLicense, spread throughout a total of 161 users. One of these passwords was used by 103 people, and is a single word of the English language that is very easy to guess. Four other passwords were each used by five or more users of eLicense. Some of these users have administrator level access to the system. In addition, 11 users had a password identical to their username.

By simply Google searching the hashes of these 17 passwords, we were able to determine the plaintext for 16 of them, resulting in our being able to log into the accounts of 155 of these 161 users. Had we used a dictionary attack or other methods upon the entire list of password hashes, we likely would have found even more, as no password length

or complexity requirements were in place, and the hashes were not salted, which is a random string of data used to modify a password hash. While we would not have had access to the hashes unless able to breach infrastructural components used by the eLicense system, many of these passwords would have nonetheless been very easy to guess. In order to avoid revealing passwords that might still be in use, we are not disclosing specific examples.

Effect: Weak password controls could compromise the system's ability to accurately authenticate users. If employees were to try to guess the passwords of others in their office, given the current state of password controls and the passwords that were in use at the time of our testing, it is likely that some would be successful.

While the eLicense administration area is only accessible from inside the state network, limiting this risk primarily to unauthorized access by state employees, the system could be particularly at risk in the event of an outside breach into the state network.

The department is not in compliance with NIST SP 800-53 controls IA-5, Authenticator Management.

Cause: The eLicense system is administered by multiple agencies without any central authoritative body governing the system as a whole.

Recommendation: The Department of Administrative Services should take steps to strengthen its password controls and advise or limit user agencies' ability to adjust the configuration of those controls. (See Recommendation 1.)

Agency Response: "DAS agrees with this recommendation. DAS has published password standards that meet the NIST controls. The system can support these features and we will work with agencies on a change management plan for current users to implement the recommended controls."

Unsuccessful Logon Attempts

Criteria: The National Institute of Standards and Technology recommends various access controls (AC) in its special publication 800-53 (SP 800-53). Control AC-7, Unsuccessful Login Attempts, requires the organization to define and enforce a limit of consecutive invalid login attempts by a user during a specified time period and automatically lock out the user for a specified time period when the maximum number of unsuccessful attempts is exceeded.

Condition: The eLicense system allows for user agencies to configure a set number of failed logon attempts after which an account is locked out. However, all agencies have configured their accounts to never be locked out regardless of how many unsuccessful logon attempts occur.

Effect: Individuals have a greater ability to gain unauthorized access to eLicense through guessing passwords or using tools to automatically attempt a large number of commonly used passwords.

Cause: The eLicense system is administered by multiple agencies without any central authoritative body governing the system as a whole.

Recommendation: The Department of Administrative Services should take steps to limit user agencies' ability to adjust the number of unsuccessful login attempts after which accounts are locked out. (See Recommendation 2.)

Agency Response: "DAS agrees with this recommendation. In February 2016 we added a restriction of lockout after 10 unsuccessful login attempts in conformance with DAS/BEST Password Standards."

Disabling of Inactive Accounts

Criteria: The National Institute of Standards and Technology recommends various access controls in its special publication 800-53 (SP 800-53). Control AC-2 (3), Account Management, Disable Inactive Accounts, requires the organization's information system to automatically disable inactive accounts after an organization-defined time period.

Condition: The eLicense system does not automatically disable inactive accounts after any defined time period.

At the time of our testing in July 2015, of the 633 accounts that were active, below was the distribution of accounts by number of years since last login:

Condition	**# User IDs**
Last used this year	386
Last used between 1 to 2 years ago	14
Last used between 2 to 3 years ago	14
Last used between 3 to 4 years ago	10
Last used between 4 to 5 years ago	12
Last used between 5 to 6 years ago	5
Last used between 6 to 7 years ago	2
Never used	190

Effect: The failure to lock out inactive accounts presents the possibility that some employees would have unneeded access to the system, leaving open excessive access to the system. It also leaves open the potential for other individuals to attempt to login as these users.

Cause: We were informed that 23 of these accounts belong to employees of the Department of Public Safety and were never assigned access roles or used because that agency had planned to use the eLicense system, but never did so.

Because user agencies create and manage their own eLicense accounts for their employees, it is possible that accounts have been created for employees who do not need access.

The eLicense system is administered by various agencies and therefore is without any one authoritative agency that controls the system.

Recommendation: The Department of Administrative Services should request that the eLicense vendor provide the ability to automatically disable inactive accounts after a defined time period in future versions of the software, or carry out such deactivations through automated comparisons of employee job statuses in Core-CT and associated employee eLicense accounts. Until such a modification has been made, agencies should be advised to routinely review reports and disable inactive accounts manually. (See Recommendation 3.)

Agency Response: "DAS agrees with this recommendation. We will work with the Licensing Steering Committee to provide agencies with the procedure and best practices regarding routine monitoring of inactive accounts. DAS will also look into a product enhancement from the vendor to automate this process. Any resulting project would be based on resources and funding. The eLicensing Steering Committee will also assess if integration with Core-CT is warranted."

Review of Audit Logs

Criteria: The National Institute of Standards and Technology recommends various access controls (AC) and audit and accountability (AU) controls in its special publication 800-53 (SP 800-53).

Control AC-2, Account Management, requires that the organization monitor the use of information system accounts.

Control AU-6, Audit Review, Analysis, and Reporting, requires the organization to review and analyze information system audit records for

indications of organization-defined inappropriate or unusual activity and for those findings to be reported to organization-defined personnel.

Condition: Neither the Department of Administrative Services nor agencies using eLicense monitor any of the audit log records generated by eLicense. Although there is a significant amount of audit records generated from the use of user privileges, those records are not reviewed by a central body or any personnel at the agencies using eLicense.

Effect: Users could carry out illegitimate transactions or other actions without oversight, especially in instances in which a transaction does not initiate workflow or workflow is initiated but all steps can be completed by the same individual.

Cause: The eLicense system is administered by multiple agencies without any central authoritative body governing the system as a whole.

Recommendation: The Department of Administrative Services should advise user agencies that audit logs generated by the eLicense system should be reviewed by appropriate staff and DAS should provide guidance to ensure the creation of procedures defining how audit log reviews are completed and documented. (See Recommendation 4.)

Agency Response: "DAS agrees with this recommendation and will work with the Licensing Steering Committee to provide agencies with the procedure and best practices to access and review logs."

Identifier Management

Criteria: The National Institute of Standards and Technology recommends various identification and authentication controls in its special publication 800-53 (SP 800-53).

IA-2 requires that the information system uniquely identify and authenticate organizational users.

Condition: Users of the state's eLicense system do not have their state employee ID numbers recorded in the system. As a result, the only way to compare eLicense users with state employees is by matching first and last names. Many state employees have the same first and last name. The system does allow email addresses to be recorded; however, at the time of our review, only 228 out of 633, or 36% of users, had an email address on file.

Effect: The ability of those involved in enterprise administration of the system

to identify which state employee is represented by an eLicense user account is inhibited, especially those who are not involved in the creation of user accounts at the agency level. In addition, without recording state employee ID numbers, it is impossible to automatically deactivate the accounts of terminated employees because records cannot be reliably matched with Core-CT, Connecticut state government's integrated human resources, payroll, and financial system.

Cause: The eLicense system is administered by multiple agencies without any central authoritative body governing the system as a whole.

Recommendation: The Department of Administrative Services should consider adding the ability for user agencies to record state employee ID numbers or require the use of state employee ID numbers in place of usernames in the eLicense system and implement a related policy. (See Recommendation 5.)

Agency Response: "DAS understands this recommendation and has confirmed that agencies have internal procedures to identify users uniquely. The Licensing Steering Committee will review the benefits of using employee ID numbers instead of usernames and evaluate the cost benefit of potential solutions. Any resulting project would be based on resources and funding."

Separation of Duties

Background: In application development, *workflow* refers to a repeatable pattern of business activity that is to be managed and controlled by the application. A simple example is a user submitting a request and the application requiring supervisor approval before that request is marked as approved within the application.

A number of steps must be completed in the eLicense system to initiate workflow prior to the completion of a transaction. User agencies have the ability to define what events trigger workflow, what steps must be completed within each workflow, and whether two or more people need to be involved, such as requiring a supervisor sign-off on the last workflow step.

Criteria: The National Institute of Standards and Technology recommends various access controls in its special publication 800-53 (SP 800-53).

Control AC-5, Separation of Duties, requires the organization to:

a) Separate [Assignment: organization-defined duties of

individuals];
b) Document separation of duties of individuals;
c) Define information system access authorization to support separation of duties.

Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. One means of accomplishing this is to divide functions among different individuals.

Condition: The Department of Administrative Services and most user agencies have no separation of duties policies.

In our review of workflows associated with active credentials, we found that a large number of workflows are currently configured in a way in which only one person can complete all actions from start to finish. In other cases, the system performs all checks on its own without manual confirmation by any person. Altogether, at the time of our testing on July 29, 2015, we found that 275,236 workflows had been completed without the involvement of two or more people.

For example, name changes of those with physician/surgeon licenses were processed by only one person on 12 occasions. Exam results for pharmacists were verified by only one person on 803 occasions. Certified public accountant licenses were issued 1,072 times, and renewals 12,382 times, by only one person. Electrical contractors were issued licenses resulting from the actions of only one person on 58 occasions. Plumbing contractors were issued licenses by only person on 28 occasions. Real estate salesperson licenses were issued by only one person on 1,937 occasions.

We were also informed by user agencies that in some cases, business processes and supervisor approvals for actions to be carried out take place outside of the system.

Effect: Allowing so many transactions to be carried out from start to finish by one employee increases the risk for illegitimate transactions to be processed, licenses to be fraudulently issued or renewed, and honest errors to go undetected.

Performing workflow steps such as supervisor approvals outside of the system does not effectively prevent illegitimate transactions or errors from occurring because individuals can carry out actions in the system regardless of what approvals may or may not have occurred outside of the system.

The department is not in compliance with NIST control AC-5, Separation of Duties.

Cause: User agencies have the ability to define what actions initiate workflow and what steps should be completed within each workflow, and whether different people need to be involved at various steps. In the instances described above, workflow triggers were not defined or were defined but configured to allow one user to complete all workflow steps.

The eLicense system is administered by multiple agencies without any central authoritative body governing the system as a whole.

Recommendation: The Department of Administrative Services should advise agencies to define workflows within the system as appropriate, develop separation of duties policies, and enforce those policies using workflow within the application. (See Recommendation 6.)

Agency Response: "DAS agrees with this recommendation. We will work with the Licensing Steering Committee to provide agencies with the procedure and best practices regarding separation of duties and enforced workflows."

Terminated Employees

Criteria: The National Institute of Standards and Technology recommends various personnel security controls (PS) in its special publication 800-53 (SP 800-53).

Control PS-4, Personnel Termination, requires the organization to disable information system access within an organization-defined time period for each instance of an employee termination. It is a good business practice for that action to be carried out on the employee's last day of work.

Condition: At the time of our testing in July 2015, we found that ten terminated employees had active user accounts in the eLicense system. Their dates of termination ranged from 2006 to 2015.

Six of these accounts, belonging to employees at the Department of Agriculture, were disassociated from their respective board, thereby indirectly making the users unable to access the system; however, the accounts, while unusable, are technically active and appear as such because they were not completely disabled. In addition, the eLicense system does not record in any audit log when users are added to or removed from boards, so we were unable to identify whether the

accounts were disabled in a timely manner.

There is some indication, through events recorded on the few related audit logs that were generated, that the employees were disabled months after termination.

One of these six employees was correctly deactivated five months after termination, but was subsequently reactivated shortly thereafter on the same day for an unknown reason, and was not correctly disabled until after our notification to the agency.

In the case of another employee, one was deactivated one month after termination, but was shortly reactivated thereafter in the same fashion. There appears to be some agency confusion as to how to deactivate accounts upon the termination of employees.

Of the remaining four user accounts, two at the Department of Consumer Protection, and two at the Department of Public Health, specific circumstances could not be determined.

It should also be noted that, because state employee ID numbers are not recorded in the eLicense system, our ability to match the population of eLicense users with terminated state employees was inhibited. Therefore, other active user accounts for terminated employees might exist, but we were unable to find them because our matching process relied on accurate spellings of employee first and last names.

Effect: Terminated employees who retain access to the system present the risk that they might inappropriately use that access, or that other individuals might try to gain access to their accounts.

The department is not in compliance with NIST control PS-4, Personnel Termination.

Cause: The eLicense system is administered by multiple agencies without any central authoritative body governing the system as a whole.

Recommendation: The Department of Administrative Services should advise agencies that all eLicense accounts should be fully locked using a defined lockout procedure upon employee termination. (See Recommendation 7.)

Agency Response: “DAS agrees with this recommendation. We will work with the Licensing Steering Committee to provide agencies with the procedure and best practices regarding the timely lock out of system access for terminated employees. Agency internal notification of personnel actions is critical to this recommendation.”

Account Management

Criteria: The National Institute of Standards and Technology recommends various access controls in its special publication 800-53 (SP 800-53).

Control AC-2, Account Management, requires that the organization:

a) Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];

b) Authorizes access to the information system based on:

1. A valid access authorization;
2. Intended system usage;
3. Other attributes as required by the organization or associated missions/business functions.

Condition: The eLicense accounts are created by administrators at each user agency. Those administrators can create and configure user accounts from start to finish on their own without supervisory approval. Creation and configuration of user accounts does not trigger any workflow involving two or more people. In addition, while the creation and configuration of user accounts is logged, user agencies informed us that this activity is not audited. User agencies also do not have any formal policies requiring that access authorizations be kept on file to substantiate that requests for access occurred prior to account creation or that appropriate approvals occurred prior to account creation or modification.

Effect: User accounts might be created unnecessarily or be configured with unnecessary privileges due to error or mischievous intentions. In addition, such errors or actions could go undetected.

The department is not in compliance with NIST control AC-02, Control AC-2, Account Management.

Cause: The eLicense system is administered by multiple agencies without any central authoritative body governing the system as a whole.

Recommendation: The Department of Administrative Services should take steps to ensure that user agencies formalize policies and procedures governing the creation and modification of user accounts, including privileges granted and revoked over time, so that the reason for any user account's

existence and its assigned privileges are documented. (See Recommendation 8.)

Agency Response: "DAS agrees with this recommendation. We will work with the Licensing Steering Committee to provide agencies with the procedure and best practices around account management including audit capability."

Least Privilege

Criteria: The National Institute of Standards and Technology recommends various access controls in its special publication 800-53 (SP 800-53). Control AC-6, Least Privilege, requires that the organization employ the principle of least privilege, "allowing only authorized accesses for users which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions."

Condition: We found that three users at the Department of Consumer Protection (DCP), one of the agencies using eLicense, had not carried out more than four actions in any year in which they used the eLicense system, despite having administrative level access to the system.

One of the three users had administrator level access to only one module; the other two had administrator level access to several modules.

Administrator accounts have the highest level privileges of all user accounts, including the ability to add and modify other user accounts. Two of these three accounts had such ability. The other account's administrative privileges were in the contact module, which would allow them to add individuals to whom credentials could be issued and modify the characteristics (name, birth date, etc.) of existing credential holders.

Effect: There is an inevitable risk that privileges might be abused by the user. For that reason, mitigating controls are put into place. However, it is a best practice, as outlined by NIST control AC-6, to assign only necessary privileges for users to conduct their jobs to eliminate this risk altogether.

The department is not in compliance with NIST control AC-06, Least Privilege.

Cause: Two of the three employees are directors and were given administrator

level access based on their job titles rather than their need to use the system. The other employee was configured with administrator level access in one module in error.

Recommendation: The Department of Administrative Services should advise user agencies to not assign extraneous privileges to users, particularly administrator level privileges, and to periodically review log data for instances in which they might have done so.

The Department of Consumer Protection and user agencies should take steps to ensure extraneous privileges are not granted to users. (See Recommendation 9.)

Agency Response: "DAS agrees with this recommendation. We will work with the Licensing Steering Committee to provide agencies with the procedure and best practices around privileges and periodic reviews."

Previous Logon Notification

Criteria: The National Institute of Standards and Technology recommends various access controls in its special publication 800-53 (SP 800-53).

Control AC-9 requires that the information system notify the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last logon.

Condition: The eLicense system does not notify the user, upon successful logon, of the date and time of the last logon, or the number of unsuccessful logon attempts since the last successful logon.

Effect: If a user's account or password were compromised, the lack of this control might delay the detection of that fact.

The department is not in compliance with NIST control AC-9, Previous Logon Notification.

Cause: The eLicense system is administered by multiple agencies without any central authoritative body governing the system as a whole.

Recommendation: The Department of Administrative Services should communicate with the eLicense vendor to ensure that future versions of the software include a notification of when the last successful logon occurred and the number of unsuccessful logon attempts since. (See Recommendation 10.)

Agency Response: "DAS understands the recommendation and will work with the Licensing Steering Committee on defining the requirements based on NIST control AC-9 guidelines. Implementation of this recommendation requires a product enhancement to be provided by the vendor. Any resulting project would be based on resources and funding."

Concurrent Session Control

Criteria: The National Institute of Standards and Technology recommends various access controls in its special publication 800-53 (SP 800-53).

Control AC-10 requires that the information system uniquely identify and authenticate organizational users.

Condition: eLicense does not limit the number of concurrent sessions. The same user account may be used on multiple computers at the same time.

Effect: If a user's account or password were compromised, the lack of this control might delay the detection of that fact.

The department is not in compliance with NIST control AC-10, Concurrent Session Control.

Cause: The eLicense system is administered by multiple agencies without any central authoritative body governing the system as a whole.

Recommendation: The Department of Administrative Services should communicate with the eLicense vendor to ensure future versions of the software limit or fully prohibit a user account from being used on multiple computers at the same time. (See Recommendation 11.)

Agency Response: "DAS understands the purpose of the control recommendation but the business model for use of system utilizes multiple sessions. Access controls provide mitigation of unauthorized access."

Lack of Written, Documented Policies and Procedures

Criteria: The Office of Policy and Management, Network Security Policy and Procedures, version 2.1, states that each agency must submit its own Network Security Policy to the Security Oversight Committee for review and approval. It also states that each agency will develop its own network security policy and that the policy will address: a) system access control, which includes how to choose passwords, how to set up passwords and log-in/log-off procedures, b) System Privileges; limiting

system access, process for granting system privileges, and the process for revoking system privileges.

Condition: Our review of management controls for the eLicense system disclosed that none of the five user agencies has any written documentation of policies and procedures related to creating, modifying, or deleting user accounts. Although they may have a procedure for creating the user, there is no documented form for approvals of the new user.

During our review of the eLicense system, we contacted the Office of Policy and Management (OPM) to determine whether the user agencies had submitted their own network security policy and whether they have submitted the policy for approval by OPM's Security Oversight Committee. OPM informed us that they have no record of any of the agencies submitting their respective network security policies. We were also informed by OPM that the Security Oversight Committee established under the previous Department of Information Technology was never sustained under that agency. As such, the Office of Policy and Management has determined that this is an outdated policy, which no longer describes the needs and operation of the state and will be scheduled for revision.

Effect: If there are no documented approvals of new or modified users, there is a risk that a rogue user could be created, which may lead to unauthorized access to confidential information.

Cause: The eLicense system is administered by multiple agencies without any central authoritative body governing the system as a whole.

Recommendation: The Department of Administrative Services should create and document formal policies and procedures to grant access to any and all users of the eLicense system. DAS should work with OPM on the revision of the Network Security Policy and ensure its participation in any such security oversight committee that may need to be established. (See Recommendation 12.)

Agency Response: "DAS agrees with this recommendation. We will work with the Licensing Steering Committee to provide agencies with minimum standards on granting access and will work with License Steering Committee on more specific policy for the eLicense system. DAS will also check if revisions are necessary to the Network Security Policy."

Lack of Risk Assessment Testing and Vulnerability Testing of the System

Criteria: The National Institute of Standards and Technology recommends

various risk assessment controls (RA) in its special publication 800-53 (SP 800-53).

Control RA-1, Risk Assessment Policy and Procedures, requires that the organization develop, document, and disseminate a risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance and procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls. In addition, Control RA-1, requires that the organization review and update the current risk assessment policy and risk assessment procedures.

Control RA-5, Vulnerability Scanning, requires that the organization scan for vulnerabilities in the information system and hosted applications and when new vulnerabilities potentially affecting the system/applications are identified and reported, that the organization employ vulnerability scanning tools and techniques to facilitate interoperability among tools and automate parts of the vulnerability management process.

Condition: Our review of management controls for the eLicense system disclosed that there has not been a risk assessment performed on the eLicense system. In addition, no vulnerability testing has been performed, either by the vendor or by the Department of Administrative Services, Bureau of Enterprise and Systems Technology (BEST).

Effect: The lack of vulnerability scanning opens the eLicense system to potential unknown vulnerabilities that may not be identified and remediated in a timely fashion.

Cause: The eLicense system is administered by multiple agencies without any central authoritative body governing the system as a whole.

Recommendation: The Department of Administrative Services should perform a risk assessment, analysis and vulnerability scanning of the eLicense system. (See Recommendation 13.)

Agency Response: "DAS agrees with this recommendation and will ensure that a risk assessment, analysis and vulnerability scanning of the eLicensing system is performed."

One additional finding has been removed from this report due to its sensitive nature. The Department of Administrative Services agrees with the finding and is currently working to correct the weakness in the system.

RECOMMENDATIONS

1. **The Department of Administrative Services should take steps to strengthen its password controls and advise or limit user agencies' ability to adjust the configuration of those controls.**

   Comments:

   We found that eLicense system lacked password controls and policies. The lack of password controls could compromise the system's ability to accurately authenticate users.

2. **The Department of Administrative Services should take steps to limit user agencies' ability to adjust the number of unsuccessful login attempts after which accounts are locked out.**

   Comments:

   We found that eLicense user agencies have configured their accounts to never be locked out regardless of the number of unsuccessful login attempts.

3. **The Department of Administrative Services should request that the eLicense vendor provide the ability to automatically disable inactive accounts after a defined time period in future versions of the software, or carry out such deactivations through automated comparisons of employee job statuses in Core-CT and associated employee eLicense accounts. Until such a modification has been made, agencies should be advised to routinely review reports and disable inactive accounts manually.**

   Comments:

   We found that the eLicense system does not automatically disable inactive accounts after any defined time period.

4. **The Department of Administrative Services should advise user agencies that audit logs generated by the eLicense system should be reviewed by appropriate staff and DAS should provide guidance to ensure the creation of procedures defining how audit log reviews are completed and documented.**

   Comments:

   We found that neither the Department of Administrative Services nor agencies using eLicense monitor any of the audit logs generated by eLicense.

5. **The Department of Administrative Services should consider adding the ability for user agencies to record state employee ID numbers or require the use of state employee ID numbers in place of usernames in the eLicense system and implement a related policy.**

   Comments:

   We found that state employee ID numbers are not associated with eLicense user accounts in the eLicense system. As a result, the only way to compare eLicense users with state employees is by matching first and last names, which is difficult because many state employees share the same name.

6. **The Department of Administrative Services should advise agencies to define workflows within the system as appropriate, develop separation of duties policies, and enforce those policies using workflow within the application.**

   Comments:

   The Department of Administrative Services and most user agencies have no separation of duties policies or defined workflows.

7. **The Department of Administrative Services should advise agencies that all eLicense accounts should be fully locked using a defined lockout procedure upon employee termination.**

   Comments:

   At the time of our testing, we found that ten terminated employees had active user accounts in the eLicense system.

8. **The Department of Administrative Services should take steps to ensure that user agencies formalize policies and procedures governing the creation and modification of user accounts, including privileges granted and revoked over time, so that the reason for any user account's existence and its assigned privileges are documented.**

   Comments:

   We found that eLicense accounts are created by administrators at each user agency and these agencies do not have formal policies requiring that the documentation of such authorizations be kept on file to substantiate the requests for access.

9. **The Department of Administrative Services should advise user agencies to not assign extraneous privileges to users, particularly administrator level privileges,**

and to periodically review log data for instances in which they might have done so.

The Department of Consumer Protection and user agencies should take steps to ensure extraneous privileges are not granted to users.

Comments:

We found that three users at the Department of Consumer Protection (DCP) had not carried out more than four actions in any year in which they used the eLicense system, despite having administrative level access to the system. Administrator accounts have the highest level privileges of all user accounts, including the ability to add and modify other user accounts

10. **The Department of Administrative Services should communicate with the eLicense vendor to ensure that future versions of the software include a notification of when the last successful logon occurred and the number of unsuccessful logon attempts since.**

Comments:

We found that the eLicense system does not notify the user, upon successful logon, of the date and time of the last logon, or the number of unsuccessful logon attempts since the last successful logon.

11 **The Department of Administrative Services should communicate with the eLicense vendor to ensure future versions of the software limit or fully prohibit a user account from being used on multiple computers at the same time.**

Comments:

We found that the eLicense system does not limit the number of concurrent sessions. The same user account may be used on multiple computers at the same time.

12. **The Department of Administrative Services should create and document formal policies and procedures to grant access to any and all users of the eLicense system. DAS should work with OPM on the revision of the Network Security Policy and ensure its participation in any such security oversight committee that may need to be established.**

Comments:

We found that there were no written policies and procedures related to creating,

modifying, or deleting user accounts. OPM also informed us that the Network Security Policy was outdated and needs to be revised

13. The Department of Administrative Services should perform a risk assessment, analysis, and vulnerability scanning of the eLicense system.

Comments:

Our review disclosed that there has not been a risk assessment performed on the eLicense system. In addition, no vulnerability testing has been performed, either by the vendor or by DAS BEST.

CONCLUSION

In conclusion, we wish to express our appreciation for the cooperation and courtesies extended to our representatives by the personnel of the Department of Administrative Services during the course of our examination.

Bruce C. Vaughan
Principal Auditor

Approved:

John C. Geragosian
Auditor of Public Accounts

Robert M. Ward
Auditor of Public Accounts