

STATE OF CONNECTICUT



*AUDITORS' REPORT
DEPARTMENT OF MOTOR VEHICLES
CONNECTICUT INTEGRATED VEHICLE AND LICENSING SYSTEM (CIVLS)
INFORMATION TECHNOLOGY SECURITY AUDIT
AS OF OCTOBER 2017*

AUDITORS OF PUBLIC ACCOUNTS
JOHN C. GERAGOSIAN ❖ ROBERT J. KANE

Table of Contents

EXECUTIVE SUMMARY	i
INTRODUCTION	1
COMMENTS	2
FOREWORD	2
STATE AUDITORS' FINDINGS AND RECOMMENDATIONS.....	4
Password Policy Control Weakness	4
Changes to User Access Levels Not Logged	5
Configuration Procedure Weaknesses	6
Lack of Access Enforcement.....	7
Reporting Database Not Denormalized.....	9
Application Assessment Concerns	10
Least Privilege Not Employed.....	11
Authentications Control.....	12
No Development or Quality Assurance Environment.....	12
Dormant Accounts Not Automatically Disabled.....	13
Terminated Employees Accounts Not Promptly Disabled.....	14
Lack of Documented Policies and Procedures	15
Lack of Risk Assessment Policy, Assessment, Testing, and Security Categorization....	16
Lack of Security Planning Policy and Procedures, and System Security Plan	18
Security Assessment and Authorization Policy and Procedures	19
Lack of IT Service Level Agreement	20
Configuration Management Policy and Procedures Not Implemented.....	21
Personnel Security Policy and Procedures Not Implemented	22
Security Awareness and Training Policy and Procedures	22
RECOMMENDATIONS	24
ACKNOWLEDGEMENT	29
CONCLUSION.....	30

EXECUTIVE SUMMARY

In accordance with the provisions of Section 2-90 of the Connecticut General Statutes, we have audited certain operations of the Department of Motor Vehicles (DMV) Connecticut Integrated Vehicle and Licensing System (CIVLS). The objectives of this review were to evaluate the department's internal controls, compliance with policies and procedures, as well as certain legal provisions, and management practices and operations for the period ending October 2017.

The key findings are presented below:

Page 5	DMV is not enforcing its password policy for Connecticut Integrated Vehicle and Licensing System (CIVLS) across all accounts having access to the system. The Department of Motor Vehicles should ensure that its intended password policy is enforced across all accounts having access to the Connecticut Integrated Vehicle and Licensing System. (Recommendation 1.)
Page 9	DMV does not test transactional data for conformance to intended business rules and assigned access authorizations. The Department of Motor Vehicles should test transactional data for conformance to intended business rules and assigned access authorizations. The department should modify the application, as needed, to properly enforce all intended business rules. (Recommendation 4.)
Page 12	The CIVLS application was developed in such a way that it does not provide the best available system security. The Department of Motor Vehicles should take steps to eliminate the need for the Connecticut Integrated Vehicle and Licensing System to use a service account with excessive permissions. DMV should then remove those permissions. (Recommendation 7.)
Page 13	CIVLS authentication controls were not set at the highest level of security. The Department of Motor Vehicles should take steps to properly implement secure authentication controls. (Recommendation 8.)
Page 15	DMV does not disable inactive accounts after any defined period or when employees terminate state service. The Department of Motor Vehicles should take steps to ensure that inactive Connecticut Integrated Vehicle and Licensing System accounts are automatically disabled after a defined period of inactivity or when employees terminate state service. (Recommendation 10. and 11.)
Pages 17-24	DMV has not developed numerous security policies and procedures for the CIVLS application. The Department of Motor Vehicles should develop these policies and procedures. (Recommendations 12. – 17.)

STATE OF CONNECTICUT



AUDITORS OF PUBLIC ACCOUNTS

JOHN C. GERAGOSIAN

State Capitol
210 Capitol Avenue
Hartford, Connecticut 06106-1559

ROBERT J. KANE

October 4, 2019

AUDITORS' REPORT DEPARTMENT OF MOTOR VEHICLES CONNECTICUT INTEGRATED VEHICLE AND LICENSING SYSTEM (CIVLS) INFORMATION TECHNOLOGY SECURITY AUDIT AS OF OCTOBER 2017

We have audited certain operations of the Department of Motor Vehicles (DMV) Connecticut Integrated Vehicle and Licensing System (CIVLS) 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 October 2017. 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 Motor Vehicles (DMV) Connecticut Integrated Vehicle and Licensing System (CIVLS).

COMMENTS

FOREWORD

The role and responsibilities of the Department of Motor Vehicles (DMV) are identified primarily under Title 14, Chapters 246 through 255 of the General Statutes. The department's principal function is the licensing and registration of drivers, automobiles, dealers, and repairers. The department also administered, through various contractors, the state's auto emissions inspection program.

DMV issued a request for proposal (RFP) in August of 2008 to modernize and consolidate many of its older legacy information technology systems. DMV contracted with Science Applications International Corporation (SAIC) in 2009 for \$26.9 million to develop the Connecticut Integrated Vehicle and Licensing System (CIVLS). SAIC later assigned the contract to 3M Corporation, which worked on the project until 2016 when DMV terminated the contract. The CIVLS project was part of a larger plan to modernize DMV operations to improve the department's overall business and administrative processes.

Under the terms of the initial CIVLS contract, the project was scheduled to be implemented through a few separate releases with a projected system completion during the fall of 2012.

DMV implemented the first releases (R1 and R1a) of the project, for the licensing process of dealers and auto repair establishments (Dealer License Manage Regulated Business) in 2012. DMV implemented the third release (R2), for vehicle registrations and titles, during the summer of 2015. To date, DMV has not implemented the fourth and final release (R3), for the modernization of the licensing system. DMV took full control of the system when the department terminated the contract with 3M Corporation in 2016.

The CIVLS project encountered significant issues during development and implementation of the system, causing extensive delays and cost overruns. The CIVLS application is a modified off-the-shelf (MOTS) software solution, which has been customized to meet the specific needs of the

department. Other state motor vehicle departments purchased this software, and encountered similar problems.

During our review of the CIVLS project, we identified numerous issues that contributed to the problems DMV encountered during the project's implementation. Our review was limited to evaluating and testing the information technology security, policies, and procedures that DMV implemented to control the CIVLS application. Below is a list of some of the significant factors:

- Insufficient scope development and the omission of certain requirements in the RFP.
- The vendor's lack of understanding of the complexity of the project and scope.
- Overly optimistic project milestones that did not coincide with the amount of work necessary to accomplish set tasks.
- Project management turnover – 3M Corporation changed project managers 12 times.
- DMV commissioner turnover – 4 different commissioners during the implementation of a major IT project.
- Scope modifications – A significant amount of modifications occurred, because both parties did not properly include and review CIVLS contract requirements.
- The DMV Internal Audit Services Unit was not involved in project planning to provide feedback on proper internal control requirements.

During the implementation of the CIVLS application, several commissioners were responsible for oversight of the project. Robert M. Ward served as commissioner from January 2007 through January 2011. Commissioner Ward served during the planning, contracting, and initial development phases of CIVLS. Melody A. Currey served as commissioner from January 2011 until January 2015. Commissioner Currey held this position during the majority of the system development phase of CIVLS. Governor Malloy appointed Commissioner Andres Ayala Jr. as DMV commissioner in January 2015, just prior to the implementation of the third release of CIVLS (R2). Commissioner Ayala resigned on January 20, 2016, and was replaced by Michael Bzdyra, who served as commissioner until January 18, 2019. On February 28, 2019, Governor Lamont announced the appointment of Sibongile Magubane as DMV commissioner who officially assumed the role on April 1, 2019.

STATE AUDITORS' FINDINGS AND RECOMMENDATIONS

Our review of the information technology control environment of the Department of Motor Vehicles CIVLS revealed certain areas warranting attention that are discussed in the following findings. Significant security details regarding our audit of the information technology security of the DMV CIVIL system have been excluded from this report and provided to the management of the Department of Motor Vehicles.

Password Policy Control Weakness

Background: Many state agencies use single sign-on user authentication to integrate user accounts on a domain with users authorized to access various applications. As such, employees do not need to maintain a username and password separate from the credentials they already use to log in to their workstations running Microsoft Windows.

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 that organizations:

- 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: The Department of Administrative Services (DAS) maintains a domain, at the enterprise level, serving the information technology needs of many state agencies and their applications. DAS delegates certain levels of control to various agencies by defining them within different organizational units, which allows them to assign users to different security groups.

DAS has a default password policy that takes effect for all user accounts on their domain in the absence of a separately defined policy.

The Department of Motor Vehicles (DMV) established a stricter password policy for DMV user accounts.

At the time of our testing on December 19, 2016, DMV had only assigned 125 CIVLS user accounts, out of over 800 DMV employees, to the stricter password policy designated for use with CIVLS. DMV assigned the remaining CIVLS accounts to the default password policy.

Effect: Because DMV did not assign user credentials to the intended stricter password policy, they are more likely to become compromised.

Cause: DMV informed us that not all users were assigned to the stricter password policy during CIVLS Release 2 go-live in August 2015 to minimize login issues. DMV also informed us that there were initially some problems with the password reset functionality.

Recommendation: The Department of Motor Vehicles should ensure that its intended password policy is enforced across all accounts having access to the Connecticut Integrated Vehicle and Licensing System. (See Recommendation 1.)

Agency Response: “This policy has been addressed. An industry standard password policy has been implemented.”

Auditors’ Concluding

Comments: DMV recently provided our office with a copy of its new policy. We will test the policy during our next audit.

Changes to User Access Levels Not Logged

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

Control AU-2, Audit Events, requires that the information system be capable of auditing organization-defined auditable events. The organization is to define those events that are significant and relevant to the security of the information system as audit events.

Control AC-2, Account Management, details several enhancements describing specific ways to implement controls related to the management of information system accounts. The fourth enhancement describes a system that “automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.” This enhancement is noted to have a moderate to high impact.

Condition: The department’s information systems audit trail does not capture changes to logical access restrictions.

Effect: DMV lacks control over inappropriate access levels being issued to and removed from users. The department lacks the ability to determine when users are added to or removed from groups, or even enabled and disabled. This impedes the ability of internal or external auditors to review the current appropriateness of access levels. It also impedes their ability to review access levels for the remainder of the audited period.

Cause: DMV did not deem the logging of changes to user access levels as a priority.

Recommendation: The Department of Motor Vehicles should expand its audit trails to include changes to user access levels in the Connecticut Integrated Vehicle and Licensing System. (See Recommendation 2.)

Agency Response: “This finding has been addressed. The logging of changes to user access levels is complete.”

Auditors’ Concluding

Comments: DMV recently provided our office with a report displaying disabled accounts, but it did not include all of the required tracking functionality. We will test the policy during our next audit.

Configuration Procedure Weaknesses

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

Control AC-2, Account Management, describes various ways of effectively managing the creation, enabling, modification, and removal of information system accounts in accordance with organization-defined procedures or conditions.

Condition: Current DMV procedures contain the following weaknesses:

- DMV does not regularly extract user information as part of a structured or routine review process.
- DMV does not link accounts to employee records. Specifically, employee ID numbers are not associated with usernames, even though an employee number attribute has been designed for this purpose.
- DMV does not log the creation of new accounts, therefore there are no such records to review.

Effect: These weaknesses have various effects:

- Minimal control preventing the administrators from creating or modifying accounts in an inappropriate or malicious manner.
- Difficulties in determining which accounts are associated with which employees. This is compounded when employees have the same or similar names or abbreviate their names.
- DMV can create new accounts without following its policies, and they can go undetected through the lack of oversight and absence of an audit trail. Additionally, intruders typically create backdoor accounts, and some malware is specifically programmed for that purpose. Because the department does not log the creation of new accounts, and consequently does not review logs of newly created accounts, there is an increased risk that intruders and malware may go undetected.

Cause: DMV did not deem logging the creation or modification of user accounts as a priority. In addition, the department’s administrators noted that they are currently in the process of working with the department’s human resources office to record current employee information for each account.

Recommendation: The Department of Motor Vehicles should take steps to improve the management of its configuration and user accounts. (See Recommendation 3.)

Agency Response: “This finding has been addressed. A procedure has been completed regarding the configuration of new, promoted/demoted, and terminated employees. The procedure also addresses the monitoring of audit log reports.”

Auditors’ Concluding Comments: DMV recently provided our office with a copy of its new policy. We will test the policy during our next audit.

Lack of Access Enforcement

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

Control AC-3, Access Enforcement, describes that an information system should enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

CIVLS was designed to respond in various ways when users attempt to perform certain edits based on their user group and types. CIVLS imposes a dollar threshold to limit the amount users are authorized to adjust before the system triggers a supervisor approval. Users do not have the same abilities, and some users have abilities that can only be carried out with a supervisor's approval.

Condition: DMV completed user acceptance testing (UAT) prior to going live with CIVLS to ensure that the system responded to various user actions as intended.

The CIVLS fee adjustment approval process was not applying the authorization thresholds for different types of users and the required supervisory approval before processing adjustments. We found the following:

- DMV examiners adjusted 12,115 fees that exceeded their \$80 authorized approval level.
- DMV examiners adjusted 193 fees that exceeded their \$150 authorized approval level.
- DMV did not review the transactional data in CIVLS after going live to ensure the system consistently enforced assigned access authorizations.

Effect: Because DMV did not review transactional data to ensure that access restrictions based on defined business rules, either preventing transactions or triggering supervisory approval, there is an increased risk that the department may not detect errors in the programming of the CIVLS application.

The supervisory approvals that were not triggered for the 12,308 transactions above resulted in less oversight for the adjustments to fees processed by examiners and non-management supervisors, and therefore, increased the risk of fraud.

Cause: DMV did not make it a priority to review transactional data for conformance to intended business rules and assigned access authorizations.

Recommendation: The Department of Motor Vehicles should test transactional data for conformance to intended business rules and assigned access authorizations. The department should modify the application, as needed, to properly enforce all intended business rules. (See Recommendation 4.)

Agency Response: “This finding has been addressed. A "New User Access" process addresses the required financial limits in the employee role templates. In addition, quarterly quality control reviews are completed to ensure compliance.”

Auditors’ Concluding

Comments: DMV recently provided our office with a copy of its new policy. We will test the policy during our next audit.

Reporting Database Not Denormalized

Background: Most modern software applications rely on relational database management systems (RDBMS) to store data. Data can be stored in multiple forms, each offering a different degree of normalization, used to speed up transaction processing.

The optimal degree of normalization depends on the primary purpose and use of the data. Generally, a transaction processing database runs optimally when the data is stored with a high degree of normalization. A reporting database runs optimally when the data is stored in a denormalized form.

Database normalization involves separating data into multiple tables, resulting in better performance when writing the data. Database denormalization involves combining related data into individual tables for reporting purposes, resulting in faster performance when reading the data.

Reporting environment data is generally populated through extract, transform, and load (ETL) processes between source transactional systems and target reporting databases. Typically, this involves the transformation of normalized tables into denormalized tables.

Criteria: DMV hired a consultant to perform an application assessment of CIVLS. The consultant offered several recommendations to improve the performance of the system’s reporting functionality.

In its report, the consultant recommended that the department evaluate whether some denormalization should occur to improve the DMV reporting or previewing of various information within the system.

Condition: The department’s reporting database is currently an identical copy of the transactional database. DMV refreshes the databases nightly. The data is not denormalized or otherwise transformed to facilitate performance or faster report views.

Additionally, tables in the reporting environment are not separately indexed to improve the speed at which reports run, which was noted in the

consultant's report.

Effect: Many reports in CIVLS run slower than they could if DMV implemented the proper optimization.

Cause: DMV has not prioritized denormalizing or otherwise transforming their transactional data to facilitate necessary reporting.

Recommendation: The Department of Motor Vehicles should review the way it stores transactional data in its databases and implements changes to improve the overall performance of the Connecticut Integrated Vehicle and Licensing System. (See Recommendation 5.)

Agency Response: "The agency agrees that CIVLS reporting should be enhanced to provide valuable data based upon the agency need. Projects regarding report optimization, and additional reporting solutions using vendor tools, are currently in progress."

Application Assessment Concerns

Background: DMV recognized the significant number of deficiencies in CIVLS and decided that it would be in the state's best interest to hire an outside consultant to perform an independent application assessment of the system. The department used the assessment to confirm known deficiencies and work with the CIVLS vendor to correct many issues.

Criteria: It would be good business practice for the department to follow up on, evaluate, and implement solutions to the security and performance concerns cited in the consultant's application assessment.

Condition: The consultant's application assessment contained 53 findings and recommendations to improve the security and/or performance of CIVLS.

Our review identified 14 findings that were not addressed elsewhere in our audit and should be prioritized by DMV. These issues have been communicated to the management of the DMV.

Effect: The effects of each of the consultant's findings varies, but the cumulative effect invariably impacts the security and performance of the system.

Cause: Many of the consultant's findings involve the CIVLS development vendor's oversights or nonconformance to industry best practices.

Recommendation: The Department of Motor Vehicles should evaluate the consultant's application assessment of the Connecticut Integrated Vehicle and Licensing System and take appropriate action to implement the findings and

recommendations. (See Recommendation 6.)

Agency Response: “The agency continues to evaluate the CIVLS system, and the consultant's application assessment, to take appropriate action to improve system functionality & security. Some of the findings referenced have been resolved or addressed with best practice standards for all new code being written.”

Least Privilege Not Employed

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

Control AC-6, Least Privilege, requires that the organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Condition: CIVLS processes transactions through a user account in the database. This account is used by applications rather than people and is often referred to as service account.

CIVLS was developed by the vendor in such a way that it does not provided the best available system security.

Effect: Application assessment to CIVLS violates the concept of least privilege.

Cause: CIVLS was developed entirely by an outside vendor. We could not determine the cause of the vendor's oversight.

Recommendation: The Department of Motor Vehicles should take steps to eliminate the need for the Connecticut Integrated Vehicle and Licensing System to use a service account with excessive permissions. DMV should then remove those permissions. (See Recommendation 7.)

Agency Response: “This finding has been addressed. DMV routinely analyzes and restricts service accounts with least privilege permissions.”

Auditors' Concluding Comments:

DMV recently provided our office with a copy of its new policy. We will test the policy during our next audit.

Authentications Control

- Criteria:* The National Institute of Standards and Technology recommends various system and communications controls (SC) in its special publication 800-53 (SP 800-53).
- Control SC-13, Cryptography Protection, governs the use of cryptography to protect information worth protecting. User passwords are worth protecting.
- Condition:* DMV authentication controls were not initially set at the highest level of security by the vendor, which would be expected for the organization.
- Effect:* This could create a security vulnerability.
- Cause:* CIVLS was developed entirely by an outside vendor. We cannot determine the cause of the vendor’s oversight.
- Recommendation:* The Department of Motor Vehicles should take steps to properly implement secure authentication controls. (See Recommendation 8.)
- Agency Response:* “This finding is currently being addressed, with a project plan in place to ensure appropriate password encryption standards are implemented by 2021.”

No Development or Quality Assurance Environment

- Background:* DMV contracted with a third-party vendor to develop each release of CIVLS. The first release addressed back office financials and common infrastructure. The second release addressed vehicle and dealer-related functionality. The third release was supposed to address driver-related functionality.
- DMV no longer plans to pursue the third release with the current vendor. The department is uncertain how or if the system can achieve equivalent, integrated functionality with the first 2 releases.
- Criteria:* The National Institute of Standards and Technology recommends various configuration management controls (CM) in its special publication 800-53 (SP 800-53).
- Control CM-3, Configuration Change Control, describes controls for the systematic proposal, justification, implementation, testing, review, and disposition of changes to the system, including upgrades and modifications.

Control CM-9, Configuration Management Plan, requires the organization to develop a configuration management plan for the information system which, among other things, describes how to move changes through the change management process and “how to control development, test, and operational environments, and how to develop, release, and update key documents.”

Condition: DMV does not have a dedicated development or quality assurance (QA) environment for CIVLS. The DMV consultant’s application assessment noted that the department currently maintains only a few different environments: production, pre-production, and user acceptance testing (UAT). Currently, the department’s development and quality assurance activities are carried out in the UAT environment.

Effect: The consultant noted that sharing a UAT environment with development and quality assurance activities does not provide the isolation DMV needs to test changes prior to user acceptance.

Cause: DMV did not prioritize the creation of an environment dedicated to development and QA activities. The importance of such an environment increased when the department acquired ownership of the code for the first 2 releases and shifted development responsibilities internally.

Recommendation: The Department of Motor Vehicles should develop a dedicated development and quality assurance environment. (See Recommendation 9.)

Agency Response: “This finding has been addressed. The agency has established all lower environments in the last quarter of 2017. These lower environments are actively being used.”

Dormant Accounts Not Automatically Disabled

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: Neither the CIVLS application nor underlying infrastructure disable inactive accounts after any defined time period.

At the time of our testing in December 2016, this is a breakdown of the number of days since each user’s last login:

Days Since Last Login	Number of Users
0 to 100	887
101-200	46
201-300	32
301-400	32
401-500	98
501+	2
Total User Accounts	1,097

Effect: The failure to disable inactive accounts may allow some users unnecessary access to the system. This results in excessive access to the system and creates the potential for other individuals to attempt to log in as these users.

Cause: DMV uses Microsoft to manage user accounts, which is not configured to automatically disable user accounts after a defined period of inactivity.

Recommendation: The Department of Motor Vehicles should take steps to ensure that inactive Connecticut Integrated Vehicle and Licensing System accounts are automatically disabled after a defined period of inactivity. (See Recommendation 10.)

Agency Response: “This finding has been addressed. Dormant accounts are monitored and deactivated when necessary.”

Auditors’ Concluding Comments: DMV recently provided our office with a copy of its new policy and a report displaying some information for disabled accounts. We will test the policy during our next audit.

Terminated Employees Accounts Not Promptly Disabled

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-04, 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 good business practice for that action to be carried out on the employee’s last day of work.

Condition: In our review of employee terminations at the department between January 1, 2015 and January 18, 2017, we found 58 instances in which an employee was terminated but the user account was not deactivated at the time of our

testing on January 19, 2017.

We were not able to perform a comprehensive review of the timeliness in which DMV disables employee user accounts upon employee termination. This is because the department does not record the employee ID associated with each user account, but only the person's name. This is problematic due to variations in spelling, misspelling, including middle names and/or initials in the first name attribute, or the use of maiden names. As a result, this review was limited in scope and aimed only to identify whether employees terminated in the past 2 years still had active accounts in CIVLS.

Effect: The failure to disable accounts belonging to terminated employees makes the department more vulnerable to intrusion, since attackers may attempt to use such open accounts.

Cause: DMV did not consistently follow its employee termination procedures.

Recommendation: The Department of Motor Vehicles should ensure that all terminated employees' Connecticut Integrated Vehicle and Licensing System accounts are fully locked using a defined lockout procedure upon their termination. (See Recommendation 11.)

Agency Response: "This finding has been addressed. A procedure has been implemented to disable terminated employee accounts within one business day."

Auditors' Concluding

Comments: DMV recently provided us a copy of its new policy and a report displaying some information for disabled accounts. We will test the policy during our next audit.

Lack of Documented Policies and Procedures

Criteria: The Office of Policy and Management (OPM) Network Security Policy and Procedures 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 that addresses: 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, a process for granting and revoking system privileges.

Condition: Our review of management controls for CIVLS disclosed that DMV does not have any documented policies or procedures related to creating, modifying, or deleting user accounts. The department does have an informal procedure for creating users.

During our review of CIVLS, we contacted OPM to determine whether DMV submitted its own network security policy for approval by the OPM Security Oversight Committee. OPM informed us that it was unaware whether DMV ever submitted a policy. After further inquiry, DMV informed us that it did not develop its own network security policy as mandated by the OPM Network Security Policy and Procedures.

Effect: DMV did not comply with the OPM network security policy. The lack of formal policies for creating, modifying, or deleting users increases the risk that a rogue user could be created. This could lead to unauthorized access to confidential information.

Cause: The DMV IT Manager informed us that he was not aware of the requirement to submit the department's network security policy.

Recommendation: The Department of Motor Vehicles should develop its own network security policy and submit it to the Office of Policy and Management's Security Oversight Committee for approval. (See Recommendation 12.)

Agency Response: "This finding is currently being addressed, with a plan in place to create written policy & procedures for network security with a target completion in December 2019."

Lack of Risk Assessment Policy, Assessment, Testing, and Security Categorization

Criteria: The Office of Policy and Management Data Classification Policy was established to adopt and apply Federal Information Processing Standards regarding data classification for all data within the custody of the State of Connecticut Executive Branch. The purpose of this policy is to ensure consistency of such data in accordance with state and federal standards, as referenced in Appendix B of the state Data Classification Methodology, which directs each executive branch agency to follow the Data Classification Methodology. The stated purpose of the Data Classification Methodology is to establish protection profiles and assign control element settings for each agency category of data for which an agency is responsible. Security Categorization is the basis for identifying an initial baseline set of security controls for the information and information systems.

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

Control RA-1, Risk Assessment Policy and Procedures, requires the organization to develop, document, and disseminate a risk assessment

policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, 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 procedures.

Control RA-2, Security Categorization, requires the organization to categorize information and the information system; document the security categorization results, including supporting rationale, in the security plan for the information system; and ensure that the authorizing official or designated representative reviews and approves the security categorization decision.

Control RA-3, Risk Assessment, requires the organization to conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification or destruction of the information system and the information it processes, stores or transmits. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations based on the operation and use of information systems. Risk assessments also take into account risk from external parties, including but not limited to, contractors operating information systems on behalf of the organization and individuals accessing organizational information systems.

Control RA-5, Vulnerability Scanning, requires the organization to scan for vulnerabilities in the information system and hosted applications.

Condition: Our review of management controls for CIVLS disclosed that DMV has not developed a formal, documented risk assessment policy, and that:

- DMV did not perform a risk assessment until approximately a year after the go-live date,
- DMV did not perform vulnerability testing until approximately a year after the go-live date, and
- DMV has not performed a security categorization of CIVLS.

Effect: The lack of a risk assessment policy, a risk assessment, and vulnerability scanning increases the risk that DMV may not identify and remediate potential unknown vulnerabilities in a timely fashion.

The lack of security categories increases the risk that DMV will be unable

to describe the potential adverse impacts to organizational operations, assets, and individuals if information and information systems are compromised through a loss of confidentiality, integrity, or availability.

Cause: It appears that DMV believed the vendor is responsible, since the vendor retained control over the CIVLS source code until recently.

Recommendation: The Department of Motor Vehicles should develop and document a formal Risk Assessment Policy and periodically perform risk assessments and vulnerability scanning to identify system weaknesses.

The Department of Motor Vehicles should also categorize the information and information system, and document the security categorization results in the system security plan. (See Recommendation 13.)

Agency Response: “This finding is currently being addressed, with a plan in place to create written policy & procedures for Risk Assessments, Vulnerability testing, and System Security Categorization. Target completion in December 2019.”

Lack of Security Planning Policy and Procedures, and System Security Plan

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

Control PL-1, Security Planning Policy and Procedures, requires the organization to develop, document, and disseminate a security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance, and procedures to facilitate the implementation of the security planning policy and associated security planning controls.

Control PL-2, System Security Plan, requires the organization to develop a system security plan for the information system that is consistent with the organization’s enterprise architecture, explicitly defines the authorization boundary for the system, describes the operational context of the information system in terms of missions and business processes, provides the security categorization of the information system including supporting rationale, and describes the operational environment for the information system and relationships with or connections to other information systems.

Condition: Our review of CIVLS management controls disclosed that the department does not have a documented security planning policy and procedures or a system security plan.

Effect: The lack of a security planning policy and procedures increases the risk that the related security controls and control enhancements may not be effectively implemented.

The lack of a system security plan increases the risk that the security controls and control enhancements may not meet security requirements.

Cause: It appears that the department believed the vendor was responsible, because the vendor retained control over the CIVLS source code until recently.

Recommendation: The Department of Motor Vehicles should develop, document, and disseminate a Security Planning Policy and Procedures; and System Security Plan. (See Recommendation 14.)

Agency Response: “This finding is currently being addressed, with a plan in place to create written policy & procedures for security planning. Target completion in December 2019.”

Security Assessment and Authorization Policy and Procedures

Criteria: The National Institute of Standards and Technology, recommends various security assessment and authorization controls (CA) in its Special Publication 800.53 (SP 800-53).

Control CA-1, Security Assessment and Authorization Policy and Procedures, requires the organization to develop a security assessment policy that addresses purpose, scope, roles, responsibilities, and procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls.

Control CA-2, Security Assessments, requires the organization to develop a security assessment plan that describes the scope of the assessment, including security controls and control enhancements under assessment, the assessment procedures to be used to determine security control effectiveness, and the assessment environment, assessment team, and assessment roles and responsibilities. Security assessments are designed to ensure that information security is built into organizational information systems to identify weaknesses and deficiencies early in the development process and to provide management with essential information needed to make risk-based decisions as part of the security authorization processes.

Control CA-7, Continuous Monitoring, requires the organization to develop a continuous monitoring strategy and implement a continuous monitoring program.

Condition: Our review of CIVLS management controls disclosed that DMV has not developed a security assessment and authorization policy and procedures.

Through inquiry, we also determined that:

- DMV has not conducted security assessments, and
- DMV has not implemented a continuous monitoring strategy and program.

Effect: The lack of a documented security assessment policy increases the risk that effective security controls and control enhancements are not properly implemented and reduces the likelihood that information security is built into organizational information systems. It also may increase the risk that the department may not identify weaknesses and deficiencies early in the development process.

Cause: It appears that DMV believed the vendor was responsible, because the vendor retained control over the CIVLS source code until recently.

Recommendation: The Department of Motor Vehicles should develop a formal Security Assessment and Authorization Policy and Procedures.

The Department of Motor Vehicles should also perform security assessments and develop a continuous monitoring strategy to facilitate ongoing awareness of threats and vulnerabilities. (See Recommendation 15.)

Agency Response: “This finding is currently being addressed, with a plan in place to create written policy & procedures for security assessments and authorizations with a target completion in December 2019.”

Lack of IT Service Level Agreement

Criteria: The Department of Administrative Services – Bureau of Enterprise Systems and Technology (DAS/BEST) provides the information technology environment to house the DMV CIVLS hardware. DMV is responsible for supporting the CIVLS software and hardware physically located in the DAS/BEST datacenter. Sound business practices dictate that agreements should be in writing to ensure the parties’ effective performance of their responsibilities in the agreement.

Condition: Through our inquiry, we discovered that the Department of Motor Vehicles and the Department of Administrative Services, Bureau of Enterprise Systems and Technology have not entered into a service level agreement

covering the DAS/BEST services and the responsibilities of both parties.

Effect: Without a service level agreement, the DAS/BEST services and the responsibilities of both parties are not properly defined, and the services delivered may be inadequate.

Cause: We were informed that a service level agreement between DAS/BEST and DMV was in draft form, and has not been formally approved.

Recommendation: The Department of Motor Vehicles should develop and execute a formal written service level agreement with the Department of Administrative Services, Bureau of Enterprise Systems and Technology, that outlines the responsibilities of both parties. (See Recommendation 16.)

Agency Response: “This finding has been addressed. An SLA was completed and signed by the previous DMV Commissioner and BEST Chief Information Officer in March 2018.”

Configuration Management Policy and Procedures Not Implemented

Criteria: The National Institute of Standards and Technology, recommends various configuration management controls (CM) in its Special Publication 800.53 (SP 800-53).

Control CM-1, Configuration Management Policy and Procedures, requires the organization to develop, document, and disseminate a configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, compliance and procedures to facilitate the implementation of the configuration management policy, and associated configuration management controls.

Condition: Our review of operational CIVLS controls disclosed that DMV does not have a documented configuration management policy and procedures.

Effect: The absence of configuration management policy and procedures increases the risk that effective security controls over changes to CIVLS may not be properly implemented.

Cause: It appears that DMV believes the vendor is responsible, since the vendor retained control over the CIVLS source code until recently.

Recommendation: The Department of Motor Vehicles should develop, document, and disseminate a formal Configuration Management Policy and Procedures. (See Recommendation 17.)

Agency Response: “This finding has been addressed. The agency developed and implemented Configuration Management procedures.”

Personnel Security Policy and Procedures Not Implemented

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-1, Personnel Security Policy and Procedures, requires the organization to develop, document, and disseminate a personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, compliance, and procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

Condition: Our review of CIVLS management controls disclosed that the department does not have documented personnel security policy and procedures.

Effect: The lack of personnel security policy and procedures increases the risk that the related security controls and control enhancements may not be effectively implemented.

Cause: It appears that DMV did not prioritize the need for a personnel security policy.

Recommendation: The Department of Motor Vehicles should develop, document, and disseminate a Personnel Security Policy and Procedures. (See Recommendation 18.)

Agency Response: “This finding is currently being addressed, with a plan in place to create written policy & procedures regarding personnel access with a target completion in December 2019.”

Security Awareness and Training Policy and Procedures

Criteria: The National Institute of Standards and Technology, recommends various awareness and training controls (AT) in its Special Publication 800.53 (SP 800-53).

Control AT-1, Security Awareness and Training Policy and Procedures, requires the organization to develop, document, and disseminate a security awareness training policy that addresses purpose, scope, roles,

responsibilities, management commitment, coordination among organizational entities, compliance, and procedures to facilitate the implementation of the security awareness and training policy and associated personnel security controls.

Condition: Our review of CIVLS management controls disclosed that the department does not have documented security awareness and training policy and procedures.

Effect: The lack of security awareness and training policy and procedures increases the risk that the related security controls and control enhancements may not be effectively implemented.

Cause: It appears that the department did not prioritize the need for a security awareness and training policy.

Recommendation: The Department of Motor Vehicles should develop, document, and disseminate a Security Awareness and Training Policy and Procedures. (See Recommendation 19.)

Agency Response: “This finding has been addressed. Mandatory online training programs, including Security Awareness Training, have been rolled out to all employees. In addition, the Training Division continues to annually monitor employee completion of DMV security training. In 2018, over 98% of employees completed the agency developed training. 2019 training is underway with target completion in October.”

RECOMMENDATIONS

1. **The Department of Motor Vehicles should ensure that its intended password policy is enforced across all accounts having access to the Connecticut Integrated Vehicle and Licensing System.**

Comments:

We found that DMV was not enforcing the intended CIVLS password control policy.

2. **The Department of Motor Vehicles should expand its audit trails to include changes to user access levels in the Connecticut Integrated Vehicle and Licensing System.**

Comments:

We found that the information system audit trail does not capture changes to logical access restrictions.

3. **The Department of Motor Vehicles should take steps to improve the management of its configuration and user accounts.**

Comments:

We found that the department does not perform regular account analysis, link accounts to employee records, or monitor new accounts.

4. **The Department of Motor Vehicles should test transactional data for conformance to intended business rules and assigned access authorizations. The department should modify the application, as needed, to properly enforce all intended business rules.**

Comments:

In our review of CIVLS enforcement of dollar adjustment thresholds, we found that users processed adjustments to fees in excess of certain dollar amounts that should have triggered supervisory approval.

- 5. The Department of Motor Vehicles should review the way it stores transactional data in its databases and implements changes to improve the overall performance of the Connecticut Integrated Vehicle and Licensing System.**

Comments:

We found that the reporting database is currently not optimized or otherwise transformed to facilitate performance or faster report views.

- 6. The Department of Motor Vehicles should evaluate the consultant's application assessment of the Connecticut Integrated Vehicle and Licensing System and take appropriate action to implement the findings and recommendations.**

Comments:

The DMV consultant's application assessment contained 53 findings and recommendations, of which we highlighted 14 significant items that have the most impact for resolving system deficiencies.

- 7. The Department of Motor Vehicles should take steps to eliminate the need for Connecticut Integrated Vehicle and Licensing System to use a service account with excessive permissions. DMV should then remove those permissions.**

Comments:

We found that the method used by the CIVLS application to process transactions could be improved to reduce excessive account permissions.

- 8. The Department of Motor Vehicles should take steps to properly implement secure authentication controls.**

Comments:

The DMV authentication controls were not set at the highest security level during our testing.

- 9. The Department of Motor Vehicles should develop a dedicated development and quality assurance environment.**

Comments:

We found that DMV does not have a dedicated development or quality assurance

environment for CIVLS.

- 10. The Department of Motor Vehicles should take steps to ensure that inactive Connecticut Integrated Vehicle and Licensing System accounts are automatically disabled after a defined period of inactivity.**

Comments:

We found that the CIVLS does not automatically disable inactive accounts after any defined period.

- 11. The Department of Motor Vehicles should ensure that all terminated employees' Connecticut Integrated Vehicle and Licensing System accounts are fully locked using a defined lockout procedure upon their termination.**

Comments:

At the time of our testing, we found that 58 terminated employees had active CIVLS user accounts.

- 12. The Department of Motor Vehicles should develop its own network security policy and submit it to the Office of Policy and Management Security Oversight Committee for approval.**

Comments:

Our review of CIVLS management controls disclosed that DMV does not have any documented policies or procedures related to creating, modifying, or deleting user accounts.

- 13. The Department of Motor Vehicles should develop and document a formal Risk Assessment Policy and periodically perform risk assessments and vulnerability scanning to identify system weaknesses.**

The Department of Motor Vehicles should also categorize the information and information system, and document the security categorization results in the system security plan.

Comments:

Our review of CIVLS management controls disclosed that DMV has not developed a formal, documented risk assessment policy.

- 14. The Department of Motor Vehicles should develop, document, and disseminate a Security Planning Policy and Procedures; and System Security Plan.**

Comments:

Our review of CIVLS management controls disclosed that DMV does not have a documented security planning policy and procedures.

- 15. The Department of Motor Vehicles should develop a formal Security Assessment and Authorization Policy and Procedures.**

The Department of Motor Vehicles should also perform security assessments and develop a continuous monitoring strategy to facilitate ongoing awareness of threats and vulnerabilities.

Comments:

Our review of CIVLS management controls disclosed that DMV has not developed a security assessment and authorization policy and procedures.

- 16. The Department of Motor Vehicles should develop and execute a formal written service level agreement with the Department of Administrative Services, Bureau of Enterprise Systems and Technology that outlines the responsibilities of both parties.**

Comments:

We found that the Department of Motor Vehicles and the Department of Administrative Services, Bureau of Enterprise Systems and Technology have not executed a service level agreement, which defines the responsibilities of both parties and the DAS/BEST services.

- 17. The Department of Motor Vehicles should develop, document, and disseminate a formal Configuration Management Policy and Procedures.**

Comments:

Our review of CIVLS operational controls disclosed that DMV does not have a written, documented configuration management policy and procedures.

18. The Department of Motor Vehicles should develop, document, and disseminate a Personnel Security Policy and Procedures.

Comments:

Our review of CIVLS management controls disclosed that DMV does not have a documented personnel security policy and procedures.

19. The Department of Motor Vehicles should develop, document, and disseminate a Security Awareness and Training Policy and Procedures.

Comments:

Our review of CIVLS management controls disclosed that DMV does not have documented security awareness and training policy and procedures.

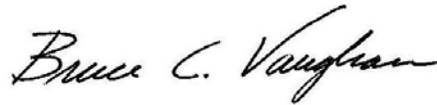
ACKNOWLEDGEMENT

The Auditors of Public Accounts would like to recognize the auditors who contributed to this report:

Michael Abbatiello
Brian DeMilia
Bruce C. Vaughan

CONCLUSION

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



Bruce C. Vaughan
Principal Auditor

Approved:



John C. Geragosian
State Auditor



Robert J. Kane
State Auditor