Texas Department of Motor Vehicles

HELPING TEXANS GO. HELPING TEXAS GROW.

# Telecommuting Program Audit Report 21 - 05

Internal Audit Division

June 2021

Texas Department *of* Motor Vehicles

# Telecommuting Program, 21-05

## Executive Summary

### BACKGROUND

The Texas Department of Motor Vehicles' (Department) telecommuting policy allowed some employees to work remotely, subject to eligibility requirements. In March 2020 the Department, in response to orders from the Governor's Office and the COVID-19 pandemic, enabled its employees to telecommute more broadly.

Each Department division adapted existing or implemented new monitoring processes to accommodate larger scale telecommuting.

Each division has developed their own telecommuting plan best suited to their business needs and may maintain a telecommuting option going forward.

The objectives of the audit were to evaluate the following:

- The Department's implementation of its telecommuting program.
- The mechanisms established to monitor remote work and telecommuting program usage.

### RECOMMENDATIONS

This report includes two low priority recommendations to reinforce usage of Virtual Private Network (VPN) by Department staff.

### RESULTS

IAD found that the processes implementing and monitoring the Department's telecommuting program are at a level 2 maturity level, Repeatable but Intuitive, where similar procedures are followed by several employees, but the results may not be consistent. The Department's telecommuting processes are not completely documented and has not been sufficiently evaluated to address risks. This rating was provided as the divisions need flexibility to monitor their remote staff based on their divisional needs and the recent changes.

Data and information gathered on operations during calendar year 2020 shows a positive impact on staff with 88% reporting better work-life balance and 70% report increased productivity. KPI data shows that process adjustments by the Department to monitor telecommuters have been as effective as monitoring done prior to large-scale telecommuting.

The Department has emphasized the importance of cybersecurity, data confidentiality, and fraud awareness when staff work from home, but has not communicated as clearly the importance of using the Department's VPN while working remotely. VPN is a key control for providing secure access to the Department's network and systems, as well as a primary delivery method for security updates to offsite computers and equipment. Though VPN usage increased over the course of 2020, the Department could reinforce VPN practice with staff.

### MANAGEMENT RESPONSE

*Management appreciates the oversight and fully agrees with the findings and is working on fully implementing both recommendations by May 21, 2021.*

# Contents

Return to Overall Conclusion

# Overall Conclusion

## Maturity Assessment Rating

2 – Repeatable but Intuitive: The function developed a process where similar procedures are followed by several employees, but the results may not be consistent. The process is not completely documented and has not been sufficiently evaluated to address risks.

Other possible ratings and definitions can be found in Appendix 1, under Maturity Assessment Rating Definition.

## Strengths

+ Divisions have established plans to implement telecommuting in their areas that helps achieve the Texas Department of Motor Vehicles (Department) goals while giving staff the flexibility to work remotely.

+ The Department has adjusted and continues to adjust its telecommuting program to help attract and retain staff.

+ Although remote work has been known to impact staff morale and organizational culture, 90% of staff surveyed felt that they still feel connected with their team's culture even when working remotely.

+ Staff overall positively support and embrace the telecommuting program and believe the Department has done an excellent job implementing the new program.

## Improvement

The Department has communicated to staff the importance of cyber security, data confidentiality, and fraud awareness when telecommuting. However, communication to staff reinforcing Virtual Private Network (VPN) usage as a key control for data security have been less prevalent.

Below are the audit results that further expand on these areas (click on the links to go directly to the result and recommendations).

- **Audit Result 1: Changes to the telecommuting program have had a positive impact on staff, but burnout is a concern.**
- **Audit Result 2: Performance monitoring has been effective in the Telecommuting Environment.**
- **Audit Result 3: Data security practices and cybersecurity threats are sufficiently managed, but staff should be reminded about using the VPN.**
    - **Recommendation 3.1**: The Department should send out another communication discussing the importance of using VPN while working remotely. **(LOW)**

Return to Overall Conclusion

- **Recommendation 3.2**: The Department should consider updating the Telecommuting Policy or Agreement to include information on the VPN. **(LOW)**

The detailed audit results can be found under the Audit Results section of this report (begins on page 4**)**.

Return to Overall Conclusion

## Background

Prior to March 2020, the Department had a telecommuting policy that allowed some employees to work remotely. At that time, the Department's experience with telecommuting varied by division with call center and divisions who frequently traveled prior to March 2020 being more experienced with working remotely. Other divisions generally had only a handful of staff doing limited basis telecommuting.

The Department waived its telecommuting policy requirements in March 2020 in response to orders from the Governor's Office and health and safety concerns of the COVID-19 pandemic, enabling more employees to work remotely. Each division made process adjustments to accommodate telecommuting, though some areas kept staff onsite where job duties required a physical presence, such as mail receiving and facilities maintenance, or where information handling was deemed too sensitive to move offsite, such as title application processing. As a result, up to 86% of Department staff were telecommuting in April 2020, and the Department maintained approximately 70% of staff regularly telecommuting through January 2021.

In anticipation to the changing environment and employee needs, the Department updated its telecommuting policy effective February 2021. The new policy eliminated previous performance and tenure eligibility requirements which extended telecommuting eligibility to more existing staff as well as new hires, subject to case-by-case division approval. With the changes to telecommuting policy, all divisions plan on maintaining a telecommuting option going forward where job duties allow. Each division has developed their own telecommuting plan that best suits their business and customer needs. These plans commonly include a hybrid onsite/offsite schedule rotating staff on a daily or weekly basis.

As more staff telecommute, the Department became more heavily reliant on communication and information systems such as email, instant messaging, and video conferencing to communicate with and monitor staff activity.

Data security and confidentiality at home workstations has been a key consideration of the Department when shifting to telecommuting operations as well as a reliance on VPN to connect to the network. The VPN provides secure access to the Department's network and information systems from external internet services and is the primary delivery method for software and security updates to computers and equipment located outside the Department's onsite network.

## Audit Engagement Team

The audit was performed by Naomi Marmell (Auditor), Frances Barker (Quality Assurance), Derrick Miller (Senior Auditor), and Sandra Menjivar-Suddeath (Internal Audit Director).

Return to Overall Conclusion

# Audit Results

## Result 1: Changes to the telecommuting program have had a positive impact on staff, but burnout is a concern.

### Condition

The Internal Audit Division (IAD) was able to identify staff perceptions and concerns with the telecommuting program. IAD surveyed staff for their thoughts on the telecommuting program, with responses reporting better work life balance and productivity when telecommuting. The telecommuting program has helped staff be more positive about the agency and the work they perform.

### Impact

IAD was not able account for direct effects of the COVID-19 pandemic, such as increased unemployment and travel restrictions, separately from the effects of telecommuting upon staff. However, the Department has been able to retain more staff in the past year. Turnover decreased from 22% to 13% between February 2020 and February 2021, and staff separations as a whole decreased by 40%.

While staff retention has increased, staff have been working more hours and taking less leave.

While the program is highly supported by Executive Management, staff did indicate that they would look for other employment if the option to telecommute was not offered.

### Cause

The Department updated its telecommuting program as a response to the COVID-19 pandemic. Through lessons learned and monitoring of performance, the Department chose to update its program to allow more flexibility. Each division created telecommuting plans specific to their staff that would allow them to work remotely while keeping key functions performing.

### Criteria

Organizations should have a culture, or control environment, that attracts, develops and retains competent individuals. The ability to attract and retain these individuals has become incumbent on having flexibility as most individuals seeking new jobs state that work-life balance is a key factor when evaluating job prospects. Having a telecommuting program that gives employees the flexibility to work remotely and reduce their stress will help the Department retain and attract qualified employees.

### Evidence

IAD collected the following evidence to produce this result:

- IAD conducted a survey of the current 565 telecommuter employees, with most of the employees being with the agency prior to the COVID – 19 response. 393 survey responses (70%) were received with the following information:

Return to Overall Conclusion

  - 95% of respondents would continue telecommuting if given the option.
  - 88% reported an improvement in work-life balance.
  - 70% reported being more productive while telecommuting.
  - 60% of employees reported that they would consider seeking other employment if they did not have an opportunity to telecommute in the future.
    - 33% of employees stated that they would certainly or probably seek other employment.
      - Employees stated they would seek other employment due to living too far from the office to make daily commuting practical and the financial and time costs of physically commuting.

Though IAD could not account for direct effects of the COVID-19 pandemic versus the telecommuting program during 2020, the following effects on Department employee leave balances were noted:

- During calendar year 2020, Department staff had an increase of 19% in combined vacation and sick leave balances, with an average increase of 2% per month, indicating that staff took less leave as the year progressed.
- During calendar year 2020, compensatory time increased by 57%.
  - In the same period, 13 of 15 (87%) divisions accrued more Compensatory and FLSA Compensatory (Comp time) than they used. Of the 15 divisions, 11 (73%) used less than 90% of the accrued time within the same year. The proportion of accrued time used in these divisions varied between 42% and 88%.

Return to Overall Conclusion

## Result 2: Performance monitoring has been effective in the Telecommuting Environment.

### Condition

Although the Department workforce has moved to a heavier telecommuting presence, staff are still being monitored to ensure Department objectives and services are being met.

### Impact

The majority of KPI performance results and divisional internal targets remained at similar levels compared to operations prior to telecommuting. This indicates that, for the most part, divisions' monitoring processes resulted in achievement of KPI targets between March 2020 and December 2020 as effectively as they did prior to March 2020.

### Criteria

The Department sets targets for Key Performance Indicators (KPIs) for individual divisions as well as the Department as a whole. KPIs address performance, output, and outcomes.

### Cause

Monitoring systems already in place were applied to or adapted for remote work and new processes were put in place to ensure performance remained the same. These include the following:

- Consumer Relations Division (CRD) conducts quality assurance reviews of phone calls and emails, and monitors staff hours.
- Information Technology Services Division (ITSD) uses ticketing queues and project task lists to ensure staff meet deadlines.
- Enforcement Division (ENF) monitors investigation outputs and deliverables.
- Compliance and Investigations Division (CID) uses a combination of remote asset pings and self-disclosures to locate TxDMV equipment at TAC offices and coordinates work through weekly meetings.
- Financial and Administrative Services (FAS) uses task logs to monitor staff workload.
- Government and Strategic Communications Division (GSC) uses regular staff meetings, shared calendars, and assigned task summaries to coordinate and monitor work.
- Motor Carrier Division (MCD) monitors staff work by monitoring staff availability on phone calls, number of permits issues, and number of compliance completed.
- Motor Vehicle Crime Prevention Authority (MVCPA) monitors workflow in its grant management tracking system and email traffic in its shared inbox for grantees.
- Office of Administrative Hearings (OAH) monitors documents and communications exchanged with customers to remain aware of deliverables provided by staff.

Return to Overall Conclusion

- Vehicle Titles and Registration (VTR) monitors daily title and registration production reports and employee transaction reports.
- Motor Vehicle Division (MVD) monitors staff through its dealer application processing reports and daily management communication on applications submitted and reviewed.

## Evidence

IAD collected the following evidence to produce this result:

- Across the Department as a whole, eight KPIs improved after the move to telecommuting, five decreased but returned to the expected range by the end of November 2020, and three decreased overall.
- Individual targets for divisions stayed about the same prior to telecommuting:
    - Motor Vehicle Division issued an average of 27,469 dealer licenses between March 2020 and December 2020. While there was an overall decrease during this period, the volume issued is commensurate with a decrease in dealer applications received, and remains comparable to previous years
    - Even though Consumer Relations Division (CRD) received an average of 8,653 emails and 54,833 phone calls per month, CRD managed to keep their quality control scores for calls and emails above 98 points with most of their staff working remotely. CRD did have an increase in not ready status during telecommuting. The average amount of not ready time per person per month was 55 hours and 38 minutes in 2019 and 58 hours and 52 minutes in 2020. However, this increase is due to the amount of time spent on answering emails.
    - CID conducted all inventory counts at Regional Services Centers and Tax Assessor Collector locations using virtual visits to inspect and identify inventory. CID located all but eight unaccountable assets across all locations.
    - VTR processed 18,731 VTR-275 requests, 4,199 military applications, and 6.6 million titles. In addition, they handled 22,865 calls.

Return to Overall Conclusion

## Result 3: Data security practices and cybersecurity threats are sufficiently managed, but staff should be reminded about using the VPN.

### Condition

Over the past year, the Department has emphasized cybersecurity through weekly messages and protected information systems while employees telecommute.

The Department has also actively monitored and mitigated incidents of cybersecurity threats even as the number of incidents has risen. While Department systems have been managing the incidents of cybersecurity threats, the Department continues to rely on VPN software to protect the network from having cybersecurity threats introduced by employees that are telecommuting and ensuring computers stay current with security and feature updates. Employees, however, are not always using the VPN when telecommuting, though there was an increase in VPN usage throughout the year.

### Impact

As telecommuting continues to be used and become more prevalent in the Department, monitoring and mitigating cybersecurity threats will continue to be important to reduce potential risk from a cybersecurity attack. In addition, employees need to be made aware of the security protocols used to protect the network and department data and equipment. Without information provided on the need for employees to use the VPN, they may not use it which could lead to data or department information being viewed by unauthorized people.

While there are circumstances where the VPN may not be needed to conduct daily work, such as employees logging into and working in a Department-approved, secure third-party hosted application, VPN continues to be needed to obtain security related patches and updates on Department software and equipment.

### Cause

While the Department has communicated cybersecurity risks and awareness to employees, it has not emphasized the use or importance of VPN as frequently. Only two messages were sent about the VPN during the past year. In addition, the updated telecommuting form and training do not discuss the need to be on the VPN when working from home.

### Criteria

Communication to staff on the importance of VPN should occur to better inform employees of the importance of VPN and how it can help mitigate cybersecurity risks.

### Evidence

IAD reviewed communication, VPN usage, and cybersecurity controls to identify the following results:

Return to Overall Conclusion

- Between November 2020 and February 2021, approximately 556 active Department employees telecommuted daily.
  - IAD estimates that 379 of 555 (68%) employees used VPN daily. IAD is providing an estimate as the number of employees using the VPN cannot be precisely determined due to reporting limitations. The VPN usage reports only capture user information when the user connects or disconnects to a VPN session. A user could be on the VPN without being reflected on the report if they maintained the same VPN session across multiple workdays.
  - The Department saw a 9% increase in VPN usage, from 369 to a maximum of 402 employees logging in to VPN daily.
- The Department uses approved third-party application security protocols and commercial antivirus and firewall applications to protect TxDMV systems and information. Although the Department saw an overall increase of 15% in email traffic and a 30% increase in cybersecurity threat events from calendar year 2019 to calendar year 2020, the Department was able to mitigate the risk:
  - Of 10,230,209 emails the Department sent and received, Department system blocked, removed, or replaced 987,008 (9.65%) that were identified as malware, phishing, or spam attempts.
  - The Department mitigated all 229 events identified, including the 70 Trojan attacks, 60 Potentially Unwanted Applications (PUA) attacks, and 28 adware attacks attempted.
- Between March 2020 and February 2021, the Department sent out 70 daily or weekly communications to employees. Out of the 70, 15 of the 70 (21%) included topics related to cybersecurity, and 6 (9%) included topics related to data confidentiality and proper equipment usage.
  - Only 1 message discussed VPN and the message was related to connecting to the VPN.
- One additional communication was sent to staff during October 2020, Cybersecurity Awareness Month, about how VPN is used to deliver security updates to agency computers.

## Recommendations

3.1 The Department should send out another communication discussing the importance of using VPN while working remotely. **(LOW)**

3.2 The Department should consider updating the Telecommuting Policy or Agreement to include information on the VPN. **(LOW)**

Return to Overall Conclusion

## Management Response and Action Plan

### Management Response & Action Plan 3.1

Management appreciates the oversight and fully agrees with the findings and is working on fully implementing recommendations 3.1   The language below has been drafted for a communication to be sent to Department staff:

> *Good Afternoon TxDMV Team,*
>
> *Remember, to help keep TxDMV systems, networks, and data cyber safe. Always connect and stay connected to the TxDMV VPN when using your Agency workstation or laptop. Using VPN will allow IT to deliver anti-virus updates and security patches, and better protect your workstation or laptop from internet attacks.*

Management Action Plan Owner: William Grote, TxDMV Chief Information Officer

Anticipated Completion Date: Completed

### Management Response & Action Plan 3.2

Management appreciates the oversight and fully agrees with the findings and is working on fully implementing recommendations 3.2.

Management Action Plan Owner: Stephanie Lopez, TxDMV Human Resources Division

Anticipated Completion Date: Completed

Return to Overall Conclusion

## Appendix 1: Objectives, Scope, Methodology, and Rating Information

### Objectives

The objectives of this audit were:

- To evaluate the Department’s implementation of its telecommuting program.
- To evaluate the Department's mechanisms established to monitor remote work and telecommuting program usage.

### Scope and Methodology

The scope of the audit included performance, employment, and operational data and employment numbers from March 2019 through February 2021.

Information and documents reviewed in the audit included the following:

- Interviews with TxDMV division directors and managers
- Survey responses self-reported from TxDMV staff
- TxDMV Key Performance Indicator results and targets
- Records of work assigned and performed
- CRD – customer call and email volume, Customer Service Representative active and not-ready codes and durations, and quality assurance scores
- VTR – number of titles and applications processed and number of calls handled
- MVD – license application production reports
- ITSD – information security threat event logs, VPN event logs, Remedyforce ticket queues, and manager assignment lists
- CID – division and county-assigned equipment inventory records
- CAPPS employee leave balance and accrual data
- Hiring and separations records
- TxDMV telecommuting policy and approval forms

This audit was included in the FY 2021 Audit Plan. IAD conducted this performance audit in accordance with Generally Accepted Government Auditing Standards and in conformance with the Internal Standards for the Professional Practice of Internal Auditing. Those standards require that IAD plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for findings and conclusions based on our audit objectives. IAD believe that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objectives.

Return to Overall Conclusion

## COSO Elements

This engagement reviewed risks and controls that were relevant to the audit objective. As part of the evaluation and testing of the risks and controls, the audit team used the following COSO components and principles as depicted in Table 1:

Table 1. COSO Elements and Principles in Scope

| COSO Element | Definition | Applicable Principles |
|---|---|---|
| **Control Activities** | The actions management established through policies and procedures to achieve objectives and respond to risks in the internal control system, which includes TxDMV's information systems. | 12 - The organization deploys control activities through policies that establish what is expected and procedures that put policies into action. |
| **Information and Communication** | The quality information TxDMV management and staff generate and use to communicate and support the internal control system on an ongoing and iterative basis**.** | 13 - The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.<br>14 - The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.<br>15 - The organization communicates with external parties regarding matters affecting the functioning of internal controls. |
| **Monitoring** | The activities establish and operate to assess the quality of performance over time. The activities include ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to effect the principles within each component, is present and functioning. | 16 -The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. |

Return to Overall Conclusion

## Report Distribution

In accordance with the Texas Internal Auditing Act, this report is distributed to the Board of the Texas Department of Motor Vehicles, Governor's Office of Budget, Planning, and Policy, Legislative Budget Board, and the State Auditor's Office. The report was also distributed to the Department's executive management team.

## Ratings Information

### Maturity Assessment Rating Definition

IAD derived the maturity assessment ratings and definitions from the Control Objectives of Information and Related Technologies (COBIT) 5 IT Governance Framework and Maturity Model and the Enterprise Risk Management (ERM) Maturity Model. The model was adapted for the TxDMV assurance audit purposes and does not provide a guarantee against reporting misstatement and reliability, non-compliance, or operational impacts. The ratings and definitions are provided in Table 2.

Table 2. Maturity Assessment Rating Definitions

| Rating | Name | Definition |
|---|---|---|
| **0** | Non-Existent | The function used no process since a standardized process is not defined or being used. |
| **1** | Initial and Ad-Hoc | The function used an ad hoc approach when issues arise because a standardized process is not defined. |
| **2** | Repeatable but Intuitive | The function developed a process where similar procedures are followed by several employees, but the results may not be consistent. The process is not completely documented and has not been sufficiently evaluated to address risks. |
| **3** | Defined | The function followed a standardized, documented, and communicated process. The process, however, may not detect any deviation due to the process not being sufficiently evaluated to address risks. |
| **4** | Managed and Measurable | The function followed a standardized, documented, and communicated process that is monitored and measured for compliance. The function evaluated the process for constant improvement and provides good practice. The process could be improved with the use of more information technology to help automate the workflow and improve quality and effectiveness. |
| **5** | Refined | The function followed a standardized, documented, and communicated process defined as having a good process that results from continuous improvement and the use of technology. Information technology was used in an integrated way to automate workflow and to improve quality and effectiveness of the process. |

Return to Overall Conclusion

## Recommendation Rating Criteria

The IAD rates audit recommendation's priority (i.e., HIGH or LOW) to help the TxDMV Board and executive management identify the importance of the recommendation. The criteria for Low and High Priority are documented in Table 3.

Table 3. Recommendation Priority Criteria

| Priority | Criteria |
|---|---|
| **Low** | • Requires only a written policy or procedure update<br>• Is within an acceptable range of risk tolerance for the Department<br>• A non-reoccurring or regulatory external audit issue |
| **High** | • Executive Management or Board Request<br>• Not within an acceptable range of the risk tolerance of the division<br>• New process had to be developed to address recommendations<br>• Regulatory impact or reoccurring issue |