WESTERN AUSTRALIA

CCC | Corruption and Crime Commission

A review of the Department of Transport's management of unlawful access to TRELIS

5 August 2021

ISBN: 978-0-6488863-7-2

This report and further information about the Commission can be found on the Commission website at www.ccc.wa.gov.au.

Corruption and Crime Commission

Postal Address	PO Box 330 Northbridge Post Shop WA 6865	**Email**	info@ccc.wa.gov.au
		Website	www.ccc.wa.gov.au
Telephone	(08) 9215 4888 1800 809 000 (toll free for callers outside the Perth metropolitan area)	**Twitter**	@CCCWestAus
		Office Hours	8.30 am to 5.00 pm, Monday to Friday
Facsimile	(08) 9215 4884		

Special Needs Services

If you have a speech or hearing difficulty, contact the Commission via the National Relay Service (NRS) on 133 677 for assistance or visit the NRS website, www.relayservice.com.au. NRS is an Australia-wide telephone service available at no additional charge. The Commission's toll-free number is 1800 809 000.

If your preferred language is a language other than English, contact the Translating and Interpreting Service (TIS) for assistance on 13 14 50. TIS provides a free, national, 24 hours a day, seven days a week telephone interpreting service. TIS also provide on-site interpreters for face-to-face interviews by contacting 1300 655 082.

TABLE OF CONTENTS

THIS PAGE HAS INTENTIONALLY BEEN LEFT BLANK

OVERVIEW

[1] The Transport Executive and Licensing Information System, known as TRELIS, is a Western Australia (WA) government owned and shared database.

[2] The Department of Transport (DoT) uses TRELIS to facilitate licensing for the State, one of DoT's main functions.

[3] Of the WA government databases, TRELIS holds the most personal information about members of the WA public.

[4] Confidential and sensitive information on TRELIS could be exploited for personal or criminal reasons.

[5] The WA community has an expectation that personal information held in TRELIS is protected, not only from external hackers, but from abuse and unlawful access by the more than 3,000 persons authorised to use TRELIS to perform official duties.

[6] The Commission undertook a thematic review of unlawful accesses to TRELIS under *Corruption, Crime and Misconduct Act 2003* (CCM Act) s 41. It considered more than 100 incidents of unlawful access to TRELIS.

[7] The review identified incidents involving improper user access to TRELIS. Some of the reasons for access included viewing of the user's own driver licence details, renewing a family member's vehicle registration, or obtaining information to share with family or friends.

[8] The review showed that DoT is reluctant to treat unlawful access to TRELIS by authorised users as serious misconduct. DoT's default position is that unlawful access is a mere conflict of interest.

[9] The Commission is concerned by this approach. Unlawful access to TRELIS is a criminal offence and is serious misconduct as defined by the CCM Act s 4.

[10] The Commission's review also identified broader concerns with DoT's management of serious misconduct risks, including a lack of basic enquiries to determine the reason for apparent improper access and inconsistency in the actions taken by DoT.

[11] This report outlines the Commission's review findings and makes formal recommendations to DoT to improve its management of the serious misconduct risks associated with the access of information in TRELIS.

[12] The Commission provided a draft of this report to DoT in accordance with s 86 of the CCM Act and received a response. The Commission has taken DoT's response into account in finalising this report.

[13] The Commission will review the actions taken by DoT to address the recommendations in 12 months' time.

BACKGROUND

What is TRELIS?

[14] TRELIS is a database used by DoT to facilitate the delivery of vehicle and driver licensing and registration services across WA.

[15] TRELIS records and stores information for this purpose. Information that users can access through TRELIS includes current and previous addresses, all vehicles owned, current contact numbers, copies of identity documents, bank account information, passports, photographs, and even some medical records. Much of the information accessible through TRELIS is personal information.

[16] DoT has set up TRELIS so that users can only obtain access to TRELIS by entering a personal password. Some information accessible through TRELIS is only accessible to some users.

What serious misconduct risks are associated with unlawful access?

[17] The serious misconduct risks associated with the unlawful access to, and use of, information held in TRELIS are known to DoT from previous Commission work in this area. They include:

- Access to personal and confidential information for personal advantage.
- Misuse of personal and confidential information for predatory reasons or the intimidation of others (vulnerable persons).
- Disclosure of personal and confidential information to another person for a corrupt purpose, such as monetary gain or criminal purposes (i.e. organised crime groups).

Who uses TRELIS?

[18] As at January 2021 nearly 3,000 users were authorised to use TRELIS, pursuant to the *Road Traffic (Administration) Act 2008* (RTA Act).

[19] Of those users, only about one third were DoT employees.

[20] The other two thirds of authorised users were external to DoT and were authorised to access TRELIS by DoT under various sections of the RTA Act.[1]

- Employees of other WA government agencies who are authorised to access TRELIS to carry out authorised functions, such as viewing licensing or registration information to fulfil their duties.
- DoT agents (local shires) and dealers (car dealers) are authorised under agreements to perform functions such as vehicle inspections or checks.
- Employees of WA Police Force, including police officers, authorised under specific delegations to perform policing duties on behalf of the Commissioner of Police, using information on TRELIS.
- The Australian Federal Police access TRELIS on a service delivery arrangement.

[21] Authorised users are required to individually sign confidentiality undertakings. The undertakings make it clear that the information contained in TRELIS can only be accessed for the purpose of performing official duties. Users are required to keep information obtained confidential.

[22] Any person who is provided access to TRELIS (a WA government owned database) for the purpose of providing a function to the WA community, is considered a public officer for the purposes of the *Criminal Code Act Compilation Act 1913* (Criminal Code) s 1.

[23] This report does not examine the risks associated with hacking or cyber attacks.

How is access to TRELIS monitored?

[24] As the owner of TRELIS, DoT is responsible for managing the serious misconduct risks associated with the unlawful access of information in TRELIS, such as the authorisation of users and, if required, cancellation of user access to TRELIS.

[25] The Driver and Vehicle Services Directorate within DoT is primarily responsible for TRELIS.

[26] Within Driver and Vehicle Services, the Business Management Team is responsible for granting access to TRELIS to users and ensuring all access requirements are met. The Governance and Intelligence Team and Investigation Services Team (IST) monitor and review the misuse of TRELIS

[1] RTA Act ss 11-12, 14.

and respond to any suspicious activity alerts. The DoT People and Organisational Development Directorate is responsible for taking action against DoT employees for any breaches of discipline.

[27] Suspicious access to TRELIS is monitored by automatic audits and alerts, which are generated when a user performs an action in TRELIS that matches one of the triggers. These are called TRELIS activity alerts. Examples of triggers include a user who searches their own name or address, or the name of someone who the user shares, or previously shared, an address with.

[28] When an alert is triggered, the access is assessed to identify whether it was made for a work related function. A DoT employee can record a note in TRELIS if they search information which may be perceived as involving a conflict of interest. This function is called client contact history. If the reason for access is unable to be confirmed, a suspicious matter report is created and sent to the IST for action.

Unlawful access to TRELIS

[29] The Criminal Code s 440A(2) states that a person unlawfully uses a restricted-access computer system if that person is not authorised to use it, or being authorised to use it, uses it other than in accordance with his or her authorisation.

[30] The Criminal Code s 440A(1) defines a restricted-access computer system as a system:

- which requires the use of a password to obtain access to the information stored in the system; and
- where the person entitled to control use of the system has taken steps to restrict knowledge of or production of the password.

[31] It is clear that TRELIS is a restricted-access computer system within s 440A because DoT has set up TRELIS so that users can only obtain access by entering a personal password.

[32] The Criminal Code s 440A(3) creates a criminal offence of unlawfully accessing a restricted-access computer system. The penalty applicable to unlawfully accessing a restricted-access computer system depends on the motives and consequences of that use.

> *A person who unlawfully uses a restricted-access computer system is guilty of a crime and is liable -*
>
> *a) if by doing so the person*

i. gains a benefit, pecuniary or otherwise, for any person; or

ii. causes a detriment, pecuniary or otherwise, to any person, of a value of more than $ 5000, to imprisonment for 10 years

b) if by doing so the person -

i. gains or intends to gain a benefit, pecuniary or otherwise, for any person; or

ii. causes or intends to cause a detriment, pecuniary or otherwise,to any person, to imprisonment for 5 years;

c) in any other case, to imprisonment for 2 years.

[33] Accessing information in TRELIS is a criminal offence if the access is not in accordance with the authorisation provided, regardless of whether the user obtains a benefit, confers a benefit, or intends to obtain a benefit or cause a detriment.

[34] The penalty for accessing a system and obtaining a benefit is greater than if the user simply accesses the system, but all unlawful accesses are criminal offences and are subject to a penalty of at least two years' imprisonment.

[35] DoT appears to take the view that no offence is committed when a person who is authorised to access TRELIS does so for purposes unconnected with a person's duties but does not obtain a personal benefit.

[36] This view is incorrect. Users are authorised to use TRELIS only for performing official duties. Access to TRELIS records for mere curiosity, without obtaining any benefit, is an unlawful use. Any unlawful use is an offence.

[37] There may be circumstances where, because a remote location is involved, an authorised user performing official duties may have little option but to access the records of a family member or close associate to carry out those duties. This may be treated as a conflict of interest. But the situation is very different from a user accessing the records of the family member or associate when not performing official functions.

[38] In addition to the offence of unlawfully accessing a restricted-access computer, a user who discloses official information without authorisation, including official information obtained from TRELIS, commits an offence of disclosing official secrets.[2] It carries a maximum term of imprisonment of three years.

[2] Criminal Code s 81.

Unlawful access is serious misconduct

[39] The CCM Act s 4 defines serious misconduct to include the commission of a criminal offence by a public officer while acting or purporting to act in his or her official capacity, for an offence which is subject to a penalty of two or more years' imprisonment.

[40] By virtue of the Criminal Code s 440A(3) **all** (emphasis added) unlawful accesses of a restricted-access computer system falls within the definition of serious misconduct in the CCM Act s 4.

[41] Unlawful access is serious misconduct even if it is unlikely that the police would bring a prosecution and even if it is unlikely a court would sentence the user to the full two years in gaol for the contravention.

[42] As a notifying authority under the CCM Act, DoT is required to inform the Commission of any reasonable suspicion of serious misconduct involving the unlawful access of information in TRELIS. That duty extends to serious misconduct by an employee of another agency.

[43] The Commission may itself investigate an allegation of serious misconduct. Alternatively, the Commission may refer the matter to DoT as the appropriate authority to conduct the investigation.

[44] When the Commission refers an allegation of serious misconduct to DoT, DoT is responsible for taking action. This includes:

- identifying if the alleged serious misconduct has occurred;
- taking disciplinary action against a public officer where appropriate; and
- implementing agency-wide changes to limit and/or prevent the same, or similar, serious misconduct from occurring.

Past investigations and inquiries

[45] In 2017, the Commission conducted a cooperative investigation with DoT and the WA Police Force.[3] The investigation identified that a DoT employee had accessed and provided confidential information obtained from TRELIS to a person suspected of dealing drugs.

[3] Corruption and Crime Commission, *Public officer caught providing confidential information to an alleged drug dealer (Case Study),* September 2017.

[46] The DoT employee was criminally charged. In October 2017, the employee was sentenced to a 12 month intensive supervision order for disclosing official information obtained from TRELIS.[4]

[47] The Commission's investigation exposed a number of serious misconduct risks in DoT's procedures and the auditability of the system. The Commission informed DoT of two specific areas of risk:

- The existence of instructions that allowed DoT staff to access details and process licenses on behalf of family and friends.
- The current system impeded DoT adequately auditing TRELIS use.

[48] In response to this incident, and as part of DoT's internal audit function, DoT engaged Ernst and Young in 2018 to audit the controls around access to TRELIS and TRELIS data.

[49] The Ernst and Young audit considered policy, procedures and practices in place for inactive accounts and inappropriate activity.[5] Ernst and Young also conducted integrity testing in which it anonymously contacted TRELIS users over the phone and asked for TRELIS log on credentials, including passwords. Almost half of the users contacted provided the information without question.

[50] Ernst and Young made six recommendations to DoT for improvements in the management of TRELIS users and for the implementation of TRELIS awareness sessions for users.

[51] In response to the Ernst and Young recommendations, DoT:

- reviewed its audit logging;
- developed a TRELIS access management presentation for staff; and
- implemented a TRELIS access management framework.

[52] However, the Ernst and Young recommendations have not been diligently implemented.

[53] In March 2021, DoT informed the Commission that the TRELIS access management presentation had not yet been delivered to any staff.

[54] The TRELIS access management framework was only implemented in December 2020, after DoT was informed of this review by the Commission.

---

[4] Corruption and Crime Commission, *Department of Transport officer guilty of unlawful use of work database (Media Release)*, 17 October 2017.

[5] Department of Transport, Ernst & Young *TRELIS Access Management Internal Audit*, November 2018, p4.

[55] The serious misconduct risks associated with the access of information in restricted-access computer systems has also been investigated by other public sector agencies and integrity agencies across Australia.

[56] In 2020, Queensland's Crime and Corruption Commission examined the improper access and dissemination of confidential information by public sector agencies in *Operation Impala - A report on the misuse of confidential information in the Queensland public sector*.

[57] Operation Impala revealed the long lasting effects on both the agency which held the information and the individuals who had their information released following the unlawful access of personal information. The operation resulted in 18 recommendations ranging from technical enhancements, support to victims and legislative amendments.

[58] In February 2020, Victoria's Independent Broad-based Anti-Corruption Commission published a *Report on unauthorised access and disclosure of public sector information held by the Victorian public sector*.

THIS PAGE HAS INTENTIONALLY BEEN LEFT BLANK

THE COMMISSION'S THEMATIC REVIEW

Conduct of the review

[59] During 2019 and 2020, over 100 incidents of unlawful access to TRELIS were notified by DoT to the Commission.

[60] On 17 July 2020, the Commission engaged with members of IST and on 30 September 2020, IST was informed of 16 matters selected for inclusion in the review. The Commission requested all documentation relevant to those matters.

[61] DoT was also asked to provide supporting documentation on each selected matter to the Commission, and some associated policy and procedures by 9 October 2020.

[62] The Commission conducted a review of each selected matter to identify what actions DoT had taken to investigate the matter and what steps, if any, had been taken to mitigate the serious misconduct risks.

[63] Of the 16 matters selected, half involved DoT employees and half were external users of TRELIS. Seven are discussed below.

Internal users

Department of Transport employees

[64] DoT is the employing authority of DoT employees. If the Commission decides to refer an allegation of serious misconduct involving a DoT employee, DoT is the appropriate authority to whom the allegation should be referred.[6]

[65] As part of the thematic review, the Commission reviewed eight matters involving DoT employees located across six Perth locations and two regional office locations.

[66] The four matters outlined below demonstrate the concerns identified as part of the Commission's thematic review.

Department of Transport employee in Business Testing

[67] Between March 2018 and October 2019, a DoT employee (DoT 1) searched, accessed and triggered TRELIS alerts 22 times. DoT 1 was based in a regional area.

[6] CCM Act s 3.

[68] The alerts were triggered because DoT 1 had the same address as the searched person's record, and shared a surname with the person searched. DoT 1 also had searched their own name and vehicle registration.

[69] IST also identified that DoT 1's partner owned a transport company.

[70] DoT considered the alerts triggered and at some point in 2019, IST referred the matter to the People and Organisational Development (POD) Directorate as a breach of the TRELIS access policy. POD took no action.

[71] On 5 December 2019, IST sent DoT 1 a written request seeking an explanation for the accesses via DoT 1's manager. The manager responded on 17 December 2019 saying that DoT 1 had been 'testing the ODT System'.[7]

[72] On 5 February 2020, IST noted the response and replied in an email to the manager stating 'should unauthorised TRELIS access be detected in the future, the matter will be referred to POD'.[8]

[73] In response to the Commission's review, DoT maintained that each access was an **'unlawful use of TRELIS'**[9] (emphasis added). However, DoT considered that because the employee 'did not reveal any corruption or intent to deceive'[10] and its investigation 'did not reveal any criminal offences or corruption',[11] the incident 'did not meet the requirements of serious misconduct'.[12] DoT concluded that the accesses were only a conflict of interest.

[74] The Commission's view is that this is serious misconduct as explained at paragraphs [39] to [44] above.

[75] The Commission's review of this matter identified a number of concerns:

- DoT's responses in relation to this matter were delayed for over a year.
- The conflict of interest between the employee and their partner's transport company was not considered by DoT. DoT did not check whether the employee had submitted a declaration for this association.

[7] Email from DoT1 to Regional Director Central, 17 December 2019.
[8] Ibid.
[9] Department of Transport, *Integrity Investigation Report* (01540/2019 & SMR2019 0142), September 2019, p 9.
[10] Department of Transport, *Report to Corruption and Crime Commission Allegations of Serious Misconduct* (01540/2019 & SMR2019 0142), 9 October 2020, p 3.
[11] Ibid.
[12] Ibid.

- There was a lack of transparency in DoT's triage and investigation process for this matter. The matter was referred to POD. POD took no action, so IST sent a letter to DoT 1.

- DoT did not conduct any enquiries. No attempt was made to ascertain the employee's role or daily duties so as to inform DoT's decision. IST did not speak to the employee. They simply sent a letter to the employee.

[76] DoT's incorrect understanding of the Criminal Code s 440A led DoT to conclude that this was merely a conflict of interest.

[77] The Commission does not understand why this particular matter was referred to POD when other similar matters were not, why POD subsequently took no action or why an employee testing a computer system uses personal or known records to test a restricted-access computer system. Given that the use of personal records for training or testing purposes is a common feature of these alerts, one solution might be to prepare a set of dummy records for training purposes and ensure any training and testing used those dummy records.

[78] Additionally, DoT failed to identify and address the serious misconduct risk of DoT 1's association with a transport company.

[79] The actions taken by DoT were inadequate and the conclusions reached were not open to be made.

A Department of Transport employee at a local driver and vehicle service centre

[80] In March and August of 2019, a customer service officer (DoT 2) working at a local driver and vehicle services (DVS) centre in Perth, searched a vehicle registration, and a day later, transferred that vehicle to themselves. (A vehicle's registration is transferred when ownership of the vehicle changes, for example it is sold or inherited.)

[81] DoT 2 also searched the records of their daughter and someone with whom DoT 2 shared an address. DoT 2 did not record a client contact history for either of the accesses.

[82] DoT reviewed the audit logs and searched social media to make a connection between the family names searched. In relation to the vehicle transferred, DoT came to the conclusion that 'this use of TRELIS for personal reasons is a breach of condition of use'.[13]

[13] Department of Transport, *TRELIS Access Assessment Investigation and Outcome*, 8 November 2019, p1.

[83] On 9 December 2019, IST sent DoT 2 a conflict of interest warning letter via DoT 2's manager. The letter was titled Notification of non-compliance with Department of Transport System Access Policy and Procedure and a list was attached of the TRELIS audit results (the triggers) for the searches in question. The letter concluded that there had been non-compliance.

[84] On 11 December 2019, DoT 2 was spoken to by their manager and handed the letter. The employee apologised and gave a verbal undertaking not to access 'inappropriate records again'.[14]

[85] On 13 March 2020, the employee resigned from DoT.

[86] In DoT's report to the Commission, pursuant to the CCM Act s 40 and dated October 2020, DoT determined that these accesses to TRELIS involved a conflict of interest. DoT relied on the fact that the employee was 'authorised to use TRELIS and had used TRELIS in accordance with (their) authorisation'.[15]

[87] The Commission does not agree with DoT's categorisation. Although DoT 2 was authorised to access TRELIS to perform official duties, DoT 2 was not authorised to access TRELIS for private purposes. The access was, therefore, an unlawful access.

[88] DoT did not consider the absence of a conflict of interest declaration by the employee. Nor did DoT consider the benefit obtained by DoT 2 in being able to view the vehicle in TRELIS before buying it.

[89] DoT failed to consider the elements of a Criminal Code s 440A offence. It treated this episode as minor misconduct even though the employee obtained a benefit in accessing TRELIS for personal reasons. This assessment by DoT is wrong. The conduct was serious misconduct.

[90] No disciplinary action was taken against the employee.

[91] The actions taken by DoT were inadequate and the conclusions reached were not open to be made.

A Department of Transport driving assessor at a local business centre

[92] In January 2018, a driving assessor (DoT 3) at a local business centre searched the records in TRELIS of a person with whom DoT 3 shared an address and in doing so, triggered TRELIS alerts. In addition, DoT 3 had been completing practical driving assessments for students of a particular driving school. The driving school was owned by DoT 3's partner.

[14] Department of Transport, *Report to the Corruption and Crime Commission Allegations of Serious Misconduct* (03116/2019 & SMR2019 0711), October 2020, p1.
[15] Ibid.

[93] On 30 May 2019, some 18 months later, DoT referred the matter to POD who assessed the allegation. DoT put the matter on hold due to an internal TRELIS review.[16]

[94] On 5 July 2019, DoT sent DoT 3 a letter of alleged breaches of its policy. DoT 3 responded stating they had completed a conflict of interest declaration form in 2014 about the relationship with the driving school owner. DoT 3 also stated that the driving assessments in question were too historic (2008 to 2017) to recall and comment on.

[95] DoT could not locate the conflict of interest form and DoT 3 did not provide a copy.

[96] On 17 September 2019, POD directed the employee to complete a conflict of interest form but took no further action.

[97] On 30 September 2020, the Commission informed DoT that this matter had been selected as part of its thematic review and requested all relevant records to facilitate the review.

[98] On 27 October 2020, POD provided a two page document to the Commission with a timeline of events which revealed more extensive suspicious TRELIS use by this employee.[17]

[99] On 24 November 2020, the Commission received a briefing note from POD stating that the matter had been re-opened after the Commission's involvement in 2020.[18]

[100] In November 2020, DoT sent a letter of allegation to the employee.

[101] As at the date of this report, no further action has been taken by POD. The matter remains ongoing.

[102] The Commission considers that the initial assessment and referral of the matter to the Commission and the internal referral to POD for action were all appropriate. However, it is not known why the allegations of unlawful TRELIS access were not progressed by POD in the first instance.

[103] The TRELIS alerts for DoT 3 spanned several years before action was taken by POD. POD later placed the matter on hold. It is not clear why action was not taken. It was only when the Commission selected this matter as part of the review that POD decided to re-open its investigation.

---

[16] Department of Transport, *Report for the Corruption and Crime Commission* (03116/2019 & SMR2019 0711), 27 October 2020, p1.
[17] Ibid.
[18] Department of Transport, *Briefing note for Managing Director: Suspected Breach of Discipline*, 24 November 2020.

[104] The Commission made multiple requests for additional supporting information from DoT during the review.[19] The information which was eventually provided lacked sufficient structure to clearly identify the sequential actions taken by DoT, including DoT's assessment of the evidence and the conclusions reached.

[105] This investigation was inadequate.

A Department of Transport employee at a regional office

[106] Between March and October 2019, a customer service officer (DoT 4) in a regional office searched in TRELIS and triggered several audit alerts. DoT 4 searched the records of family and friends with whom they shared an address. DoT 4 also accessed their own record.

[107] DoT treated the accesses of information in TRELIS as a conflict of interest.[20]

[108] On 9 December 2019, IST sent the employee (via their manager) a conflict of interest warning letter titled Notification of non-compliance with Department of Transport System Access Policy and Procedure.[21]

[109] On 13 December 2020, the manager met with DoT 4 and gave them the letter. The manager responded to IST on 13 December 2020, stating the employee house sat for the person searched over two years ago and when the person presented at the counter, the employee conducted both marine and DoT functions at the same time.[22] (Marine and licensing regulation in WA is also a function of DoT; in regional areas, a customer service officer may fulfil both of these functions).

[110] DoT 4 accessed their own records to train other employees in the office, as the systems in place were new. DoT 4's manager later reminded DoT 4 of their responsibilities and to be more attentive when serving people that they know.

[111] DoT did not inquire about the employee's role in a regional office. IST did not contact the employee directly.

[112] DoT issued the warning letter to DoT 4 (via the manager) before considering DoT 4's explanation. In doing so, DoT did not give DoT 4 procedural fairness.

---

[19] Emails between Department of Transport and Corruption and Crime Commission's Oversight Team, 9 October, 12 October, 29 October 2020.

[20] Department of Transport, *Report to the Corruption and Crime Commission Allegations of Serious Misconduct* (03288/2019, 03589/2019 & SMR2019 0739 …), October 2020.

[21] Department of Transport letter*, Notification of Non-Compliance with Department of Transport System Access Policy and Procedure*, 9 February 2019.

[22] Email from Customer Services Manager, Regional Services to Integrity DoT, 13 December 2019.

[113] DoT did not investigate whether a conflict of interest declaration had been submitted nor whether information had been disclosed.

[114] The investigation and response by DoT were inadequate. It suggests DoT considers every unlawful TRELIS access a conflict of interest, regardless of the circumstances of the case.

[115] The Commission recognises the constraints faced by employees working in small regional locations, who at times, may be the sole DoT operator. However, DoT need to ensure appropriate processes are in place to mitigate this issue.

External users

[116] As part of the thematic review, the Commission reviewed eight matters concerning the actions of external users of TRELIS.

[117] External users of TRELIS include:

- DoT agents which includes local shires, community centres, federal government agencies and private organisations;
- public officers at other WA government agencies; and
- sworn and un-sworn officers of the WA Police Force and of the Australian Federal Police.

[118] DoT authorise external users to access TRELIS for the purpose of either fulfilling functions on behalf of DoT or in support of the functions of the external user's agency.[23]

[119] Three examples of misuse of TRELIS by external users are discussed below.

A Department of Transport agent at a local shire office

[120] Between March 2019 and March 2020, a customer service officer (EU 1) at a local shire office in the mid-west region of WA, searched in TRELIS the names of family and friends with whom they had shared an address. In doing so, EU 1 triggered eight audit alerts. EU 1 processed a driver's licence application for one of the persons searched.

[121] DoT reviewed the audit logs and searched for a connection on social media. DoT could not determine if EU 1 had any relationship with the persons searched in TRELIS or with the holder of the driver's licence.

[23] RTA Act ss 11-12, 14.

[122] DoT considered the remoteness of the location and decided there was insufficient evidence to conclude that there had been serious misconduct. DoT assessed the matter as a conflict of interest.[24]

[123] On 2 June 2020, a member of IST contacted EU 1 by telephone and gave a verbal warning to EU 1, reminding EU 1 of their obligations when using TRELIS. EU 1 agreed to refrain from accessing records where there was a conflict of interest.

[124] In its report to the Commission, DoT concluded that EU 1 was authorised to use TRELIS and had accessed TRELIS in accordance with their authorisation.[25]

[125] The Commission recognises the challenges of DoT agents working in remote regional areas and the potential for increased interactions with members of the public who are known to them and which may, therefore, be perceived as giving rise to a conflict of interest. However, the Commission was unable to see how DoT determined that this matter was a conflict of interest in the absence of any further enquiries.

[126] The Commission's review identified concerns about the actions taken by DoT. DoT spoke with the external user and gave a verbal warning.

[127] However, DoT is not the employing authority of a local government employee. DoT is not authorised to take disciplinary action against EU 1. DoT should have referred this matter, including the audit logs, to the appropriate authority for action. In this case, the appropriate authority was the CEO of the local shire. The Commission is not aware of whether DoT told the local shire CEO of this matter.

[128] No consideration was given to the suspension or cancellation of EU 1's access to TRELIS.

[129] The Commission's review considers the conclusions reached by DoT were not open to be made. Further investigations should have been carried out before conclusions were reached and acted on. DoT's response was not appropriate.

A Department of Transport agent at a federal government agency

[130] From July 2018 to April 2020, an employee (EU 2) of a federal government agency triggered eight audit alerts, when searching records in TRELIS. Under the arrangements with the federal government agency, employees of that authority were entitled to access TRELIS for the agency's purposes.

[24] Department of Transport, *Report to Corruption and Crime Commission: Allegations of serious misconduct*, (03588/2019 & SMR2019 0202…) 9 October 2020.
[25] Ibid.

[131] EU 2 accessed the details of persons with whom they had shared an address and searched car registrations of known associates or family members. EU 2 was based in a remote location.[26]

[132] DoT reviewed the audit triggers and addresses searched.

[133] On 26 May 2020, IST telephoned EU 2 and gave a verbal warning about their obligations in relation to TRELIS use.

[134] DoT assessed the relationship between EU 2 and the people searched as family relationships. Based on this information alone, DoT determined there was insufficient evidence to proceed with further investigations and that an assessment of conflict of interest was appropriate.[27]

[135] As discussed above, if EU 2 accessed family member's records out of curiosity, this is unlawful access. DoT should not assume that the members of EU 2's family consented to EU 2 accessing their records.

[136] Even allowing for the remote regional location, it is not clear how DoT could have concluded that this matter was a conflict of interest without having made further enquiries.

[137] It remains unclear what authority DoT had to give a verbal warning to EU 2 and whether the federal government agency was informed of the improper use of TRELIS by one of its employees.

[138] In this instance, DoT should have referred the matter to the federal government agency or the WA Police Force for action. DoT did not consider suspension or cancellation of EU 2's TRELIS access.

[139] The Commission's review considers the conclusions reached by DoT were not open to be made and the actions taken inadequate.

A user at a state government agency

[140] On 18 and 19 September 2019, a user (EU 3) at another WA government agency searched TRELIS for a person with whom they had shared an address and a vehicle registration, triggering two audit alerts.

[141] On 30 April 2020, DoT identified that EU 3 was married to the person accessed in TRELIS. Further, the vehicle registration searched belonged to a relative of the spouse. The vehicle was later transferred to the spouse's name by EU 3, as the spouse was the beneficiary of a deceased estate.[28]

---

[26] Department of Transport, *Report to the Corruption and Crime Commission Allegations of Serious Misconduct* (03603/2019 & SMR2018 0381, SMR2018 0529…), October 2020.
[27] Ibid.
[28] Department of Transport, *Report to the Corruption and Crime Commission Allegations of Serious Misconduct* (03578/2019 & SMR2019 0800…), October 2020.

[142] On 27 August 2020, IST contacted EU 3's manager at the government agency (via email) and provided the manager with an investigation brief outlining the suspected unlawful accesses by their staff member. DoT's investigation brief listed the allegations for the unlawful accesses as substantiated.[29]

[143] DoT treated the matter as a conflict of interest and not serious misconduct because it did not consider that the conduct amounted to a criminal offence or corruption and EU 3 was authorised to use TRELIS and did so in accordance with their authorisation.[30]

[144] On 11 September 2020, the manager responded to IST via email. The manager stated that EU 3:

- did not deny the accesses and had provided possible reasons for the accesses, including curiosity;
- promised to use TRELIS 'for work purposes only'[31] in the future; and
- had health issues and valued their employment.

[145] DoT referred the matter to EU 3's agency. DoT informed the agency that the access to TRELIS was a conflict of interest.

[146] No disciplinary action was taken by the user's agency.

[147] While it was appropriate for DoT to refer the matter to the external user's agency for action, the Commission was unable to see how DoT concluded the incident to be a conflict of interest.

[148] EU 3 accessed TRELIS to search and transfer a vehicle registration into their spouse's name. The spouse should have attended a DoT DVS centre to have this transaction completed. The access and subsequent transaction by EU 3 appears to have been done for a personal reason. This is serious misconduct.

[149] DoT did not suspend or revoke, or consider suspending or revoking the user's access to TRELIS.

[150] The Commission considers that the actions taken and conclusions reached by DoT were not open to be made and that the investigation was inadequate.

---

[29] Department of Transport, *Integrity Investigation Report* (SMR2019 0800 & SMR2019 0831), 27 August 2020.

[30] Department of Transport, *Report to the Corruption and Crime Commission Allegations of Serious Misconduct* (03578/2019 & SMR2019 0800…), October 2020.

[31] Email from other government agency to Integrity at DoT, 11 September 2020.

Summary

[151] The seven matters discussed above are examples. In all 16 matters reviewed by the Commission, DoT did not pursue adequate lines of enquiry, procedural fairness was not provided to all users and conclusions reached were not open to be made.

THIS PAGE HAS INTENTIONALLY BEEN LEFT BLANK

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

[152] The review highlighted five particular areas of concern with DoT's management of TRELIS:

- DoT failed to recognise that authorised access to TRELIS may amount to unlawful access to a restricted-access computer system.
- The nature and number of TRELIS activity alerts potentially limiting their value.
- Investigation of and responses to unlawful use of TRELIS by DoT employees and external users of TRELIS were inadequate. Conclusions reached were not open to be made.
- Mechanisms for dealing with external users of TRELIS were inadequate.
- DoT's lack of positive action.

[153] In light of these matters, the Commission has made a number of recommendations which are set out at paragraph [184].

Unlawful access

[154] DoT does not accept that accesses to TRELIS which are not in the course of a user performing official duties, are outside the scope of the authority given to the user and are therefore unlawful.

[155] DoT's position is not correct.

[156] It is not consistent with legislation, nor is it in the interest of the public whose personal details are potentially accessed and disclosed.

[157] Unlawful access to information in TRELIS facilitates other more serious criminal behaviours, such as organised crime or stalking. DoT should consider referring matters involving the unlawful access to TRELIS to the WA Police Force.

[158] Agencies which are provided with access to TRELIS are not made aware of the seriousness of unlawful access to TRELIS. Clear awareness of these risks is required to build a culture of understanding and zero tolerance for the unlawful access to information.

TRELIS activity alerts

[159] DoT has over 100 automatic TRELIS activity alerts. They range from living on the same street as someone years ago, to sharing a PO Box, or sharing the same surname.

[160] While automatic alerts provide DoT with a level of awareness of potential unlawful access to TRELIS, excessive alerts can reduce their value.

[161] For example, the number of alerts triggered for a user living on the same street as someone may be significantly higher in smaller regional areas, compared to more densely populated metropolitan areas. In the seven matters detailed in this report, more than one TRELIS activity alert was triggered for each user. This fosters complacency.

[162] TRELIS activity alerts need to be contemporary and meaningful.

[163] In response to a draft copy of this report, DoT acknowledged that the TRELIS alerts trigger a high number of false positives and the need to continue to refine its alerts.

Investigations

[164] The Commission's review identified a number of broad concerns in the actions taken by DoT in respect of DoT employees. For each matter:

- DoT took some time, after the first alert, before conducting enquiries (ranging up to years).
- For all matters, DoT relied on audit alert results alone and did not ascertain what the user's roles and duties were.
- There was no consistent evidence based approach to assessing and investigating matters.

[165] Having reviewed the identified incidents, the Commission considers that DoT actions taken were inadequate and the conclusions reached were not open to be made.

[166] The Commission accepts that there will be occasions when an authorised user performing official duties is required to access information about a person with whom the user has a personal relationship. This issue is more likely to arise with users providing services on behalf of DoT, in regional and remote locations.

[167] DoT must have appropriate governance strategies in place for all users of TRELIS, especially those in regional and remote locations, to record any perceived conflicts of interest at the time of access.

[168] DoT's action usually involved an email to the user's manager or a verbal warning to the user from the other agency.

[169] DoT needs defined processes for the assessment and investigation of any authorised access to TRELIS.

Management of external users

[170] The volume of external users authorised to access TRELIS creates the potential for serious misconduct to occur. It is critical to appropriately manage who is provided access and who keeps access.

[171] As the owner of TRELIS, DoT must take action into and manage the risks of misuse of TRELIS by external users.

[172] The review found that, where there was misuse of TRELIS by external users, DoT itself reached conclusions about that misuse and acted directly in respect of it. While recognising that DoT has ultimate responsibility for the integrity of TRELIS, DoT did not refer matters to the employing authority of the external user for action.

[173] When the misuse is by an employee of another WA government agency, the misuse may amount to serious misconduct within the CCM Act. However, DoT cannot take disciplinary action directly against employees of an external user.

[174] DoT should notify the employer of the relevant user, so that the employing authority can take disciplinary action.

[175] DoT should consider reporting the matter to the WA Police Force.

[176] DoT should also take appropriate action under the arrangements by which TRELIS is made available. The most obvious form of action is to suspend or cancel TRELIS access for the particular user. Where DoT has contacted external users about unlawful use of TRELIS, it does not appear to have taken any other steps in relation to unlawful access by external users.

[177] DoT has acknowledged the need to consider suspension of user access pending the review or investigation of a matter.[32]

[32] Department of Transport, *s 86 response*, 21 June 2021.

The need for action

[178] DoT's lack of action in respect of unlawful access of information in TRELIS promotes a culture of acceptance of the use of TRELIS for personal reasons. In the absence of any findings of serious misconduct and any disciplinary action, there is no deterrent for users to refrain from accessing TRELIS for personal or other unlawful purposes.

[179] During engagement with the Commission, DoT alluded to the constraints on effectively managing the risks associated with TRELIS, given the geographical landscape of WA. It contended that it was unable to remove TRELIS access for users in remote regional areas and referred to the political constraints associated with the need of other agencies to use and access TRELIS.

[180] The Commission accepts that there is a need to provide access to TRELIS in remote locations where TRELIS users are more likely to need to deal with persons with whom they share a house or to whom they are related. The Commission considers that this difficulty would be ameliorated by a clearly enforced conflict of interest policy and for remote users to clearly identify in advance, persons with whom they deal.

[181] DoT has made some changes to policy and procedures in response to the Commission's review. DoT implemented an updated TRELIS access framework in December 2020 and conducted a series of presentations to DoT employees.[33] However, DoT must do more to ensure a consistent approach and effective messaging to all users that any unlawful access of information in TRELIS will not be tolerated.

Commission referrals

[182] As a result of this review, the Commission has amended its position on the referral of serious misconduct allegations for action.[34]

[183] For matters where the Commission forms a reasonable suspicion of serious misconduct for the unlawful access of information in TRELIS and the user is from an external agency (but still within the WA government), the Commission will consider referring the allegation to one or more appropriate authorities:

- DoT, which can consider the suspension or revoking of an individual's access to TRELIS;

[33] Department of Transport*, s 86 response*, 21 June 2021.
[34] CCM Act s 33(1)(c).

- The employing authority of another government agency which can take disciplinary action against the employee;[35]
- The Commissioner of the WA Police Force; and
- The CEO of a local government authority who can consider dismissal of the employee.

Recommendations

[184] The Commission recommends DoT:

1. Implement TRELIS policy and procedures that:
    a) appropriately acknowledge the criminality of unauthorised access to TRELIS;
    b) clearly define the processes for recording conflicts of interest (including by external users); and
    c) stop the use of records (of the user or of persons known to the user) in training or testing.
2. Implement consistent triage and investigation processes for any suspected unlawful access of TRELIS for all user groups, including federal government agencies. Where appropriate, this should include consideration of the suspension or cancellation of access to TRELIS.
3. Review current TRELIS activity alerts to ensure they are contemporary, focused, and effective.
4. Review current authorisations for TRELIS access and ensure memorandums of understanding (MOU's) are in place for all external users. The MOU's should define who the employing authority is and therefore, responsible for taking any disciplinary action and facilitating appropriate sanctions against users and the relevant agency.

[185] The Commission proposes to report on the implementation of these recommendations in 12 months' time.

[35] *Public Sector Management Act 1994* s 5.