

Report into the Misuse of a WA Police Information System

20 May 2025



ISBN: 978-1-7637189-6-8

©2025 Copyright in this work is held by the Corruption and Crime Commission (the Commission). Division 3 of the *Copyright Act 1968* (Cth) recognises that limited further use of this material can occur for the purposes of 'fair dealing', for example, study, research or criticism. Should you wish to make use of this material other than as permitted by the *Copyright Act 1968* please write to the Commission at the postal address below.

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 Telephone: (08) 9215 4888	Email: info@ccc.wa.gov.au Website: www.ccc.wa.gov.au Twitter: @cccWestAus Office Hours: Monday to Friday 8.30 am to 5.00 pm
---	--

Special Needs Services

If you have a speech or hearing difficulty, contact the Commission via the National Relay Service (NRS) on 133 677 and ask for (08) 9215 4888, or visit the NRS website, www.relayservice.com.au.

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



Image credit: This artwork was painted by Corruption and Crime Commission staff under the guidance of Justin Martin from Djurandi

INTRODUCTION	1
The Commission's investigation	1
WA Police's initial investigation by IAU	2
The further investigation by Major Crime	2
The further referral to the Commissioner of Police	3
The Commission's approach following the reallocation of WA Police's investigation to Major Crime	3
The Commission's decision	3
CHAPTER ONE	5
The unauthorised use of restricted-access computer systems	5
The Police Force Regulations	5
WA Police policies on the use of a RACS	6
The Code of Conduct	7
The underlying policy	7
Conflicts of interest	8
CHAPTER TWO	10
The background to the IAU investigation	10
The notified allegations and the Commission's Audit	11
The initial WA Police investigation	12
The further audits of Officer A's access of IMS	13
The further reports	14
CHAPTER THREE	16
Officer A's admissions	16
The circumstances surrounding Officer A's access of IMS	16
Officer A's explanations	17
Disclosure	18
Officer A's knowledge of WA Police RACS policies	19
CHAPTER FOUR	21
Officer A's unauthorised access	21
Disclosure of information	21
Serious misconduct	22
The initial investigation by IAU	23
Conclusion	24

INTRODUCTION

The Commission's investigation

- [1] This report concerns the serious misconduct of a senior police officer. His name has been suppressed to protect the identity of persons with whom he has had a close association and who are necessarily referred to in this report. The police officer will be referred to as Officer A.
- [2] Officer A is an experienced police officer, having joined the Western Australian Police Force (WA Police) in about 1986.
- [3] He has held the substantive rank of Detective Senior Sergeant (DSS) since 2007, but has acted as Detective Inspector for long periods and, on occasions, as Detective Superintendent.¹ He has been attached to the Arson Squad, the Organised Crime Squad, Police Complaint Administration, the Homicide Squad, Major Crime, the Management Audit Unit (MAU) and the Internal Affairs Unit (IAU).
- [4] In October 2022, Officer A accessed the WA Police Incident Management System (IMS) for what he admits was a personal reason. He was a member of IAU at the time.
- [5] IMS is a restricted access computer system (RACS). It is an offence to unlawfully use a RACS: *Criminal Code* s 440A.
- [6] WA Police policy prescribes the circumstances in which a police officer is authorised to use a WA Police RACS. It is a breach of the policy to access a RACS for reasons not connected with the performance of police duties.
- [7] Officer A's access of IMS in October 2022 was identified by IAU in early December 2023. Pursuant to *Corruption, Crime and Misconduct Act* 2003 (CCM Act) s 28, WA Police notified the Commission of Officer A's possible misconduct.²
- [8] The Commission decided to investigate the possible unauthorised use of IMS by Officer A (Operation Williamstown). The Commission conducted a further audit of Officer A's use of IMS (the Commission's Audit). The Commission's Audit identified other occasions on which he had accessed IMS for what appeared to be personal rather than operational reasons.
- [9] Officer A was examined by the Commission on 26 August 2024. He admitted accessing IMS on the occasions identified in the Commission's

¹ Exhibit 0024.

² The notification was made on 19 December 2023. WA Police also notified the Commission of a related allegation.

Audit. He accepted that his access had been for personal rather than operational reasons.

- [10] The Commission also concluded from evidence obtained during Operation Williamstown that, in addition to unlawfully accessing IMS, Officer A had disclosed some of the accessed information to another person who was not a member of WA Police. Unauthorised disclosure of information recorded in a RACS is contrary to WA Police policy.
- [11] Unauthorised disclosure of information accessed on a RACS may also constitute an offence contrary to *Criminal Code* s 81. An unauthorised disclosure is a disclosure by a person who is a public servant of 'official information' in circumstances where the person is under a duty not to make the disclosure. 'Official information' is information which comes to the knowledge of, or into the possession of a person, because the person is a public servant.

WA Police's initial investigation by IAU

- [12] On 19 December 2023, a senior officer in IAU was directed to investigate Officer A's access of IMS in October 2022. That direction was given on the same day as WA Police notified the Commission.
- [13] In February 2024, the senior officer recommended that WA Police exercise a discretion not to prosecute Officer A for a possible breach of *Criminal Code* s 440A. That recommendation was endorsed by a superior ranking officer.
- [14] The Commission was concerned about the adequacy of IAU's investigation and the recommended outcome, partly as Officer A was a member of IAU and partly, because the recommended outcome did not appear to fully reflect the policy reasons for restricting the use of a WA Police RACS to legitimate (that is, authorised) operational purposes.

The further investigation by Major Crime

- [15] A further audit of Officer A's access of IMS was undertaken by WA Police on about 1 August 2024 (the WA Police Audit). That disclosed other instances of access apparently for personal reasons.
- [16] It was decided to reallocate the WA Police IAU investigation to a senior investigator in the Major Crime Division. The Commission was aware of the decision at the time Officer A was examined but not of the scope of any further investigation.

- [17] The senior investigator concluded that Officer A's conduct was more serious than had been assessed by IAU. He recommended a referral to the Independent Review Panel (IRP). Officer A was stood down in the interim.
- [18] The senior investigator's recommendation was endorsed by a superior ranking officer and an IRP hearing was held on 10 October 2024. The IRP concluded that Officer A should be referred to a hearing under *Police Act 1892 s 23* (s 23 hearing).

The further referral to the Commissioner of Police

- [19] The s 23 hearing was to have been held on 28 January 2025. However, the matter was further reviewed and a decision was made to refer Officer A to the Commissioner of Police for consideration of a loss of confidence process. This process is ongoing at the time of writing.

The Commission's approach following the reallocation of WA Police's investigation to Major Crime

- [20] The Commission decided it would not further investigate Officer A's conduct of allegedly accessing IMS on the additional occasions identified in the WA Police Audit. The Commission was satisfied that WA Police had taken appropriate steps to investigate Officer A's conduct once the investigation had been reallocated to Major Crime.
- [21] Accordingly:
- a. the findings and opinions stated in this report are based on the Commission's investigation into Officer A's conduct in accessing IMS on the occasions identified in the Commission's Audit; and
 - b. the Commission has considered the reallocated investigation solely for the purpose of determining whether its investigation should be extended to include the conduct apparently disclosed by the WA Police Audit.

The Commission's decision

- [22] The Commission has formed an opinion of serious misconduct. Officer A's access of IMS on the occasions identified in the Commission's Audit, and his disclosure of at least some of the information acquired, was unauthorised and contrary to the *Police Force Regulations 1979* (the Regulations) and the WA Police Code of Conduct and RACS policies.
- [23] An opinion of serious misconduct expressed by the Commission is not a finding of serious misconduct and is not to be taken as a finding that a person has engaged in serious misconduct. Further, the Commission has

not made a finding about whether Officer A committed a criminal offence by reason of the matters considered in this report.³

- [24] This report refers to persons who are closely associated with Officer A. It is not appropriate for their identities to be publicly disclosed. Accordingly, it has been necessary to suppress the identity of Officer A.

³ Section 217A(2) of the CCM Act provides that the Commission must not publish or report a finding or opinion that a particular person is guilty of or has committed a criminal offence.

CHAPTER ONE

The unauthorised use of restricted-access computer systems

- [25] A RACS for the purpose of *Criminal Code* s 440A is a computer system that is password protected. Gaining access to information stored in a RACS or operating the system in some other way constitutes a 'use' of a RACS. As previously noted, IMS is a RACS.
- [26] The punishment prescribed for the offence created by s 440A varies according to the circumstances in which it was committed but it is punishable by at least two years imprisonment if prosecuted on indictment. The penalty for an offence against *Criminal Code* s 81 is imprisonment for three years where the offender is prosecuted on indictment.
- [27] Sections 81 and 440A were added to the *Criminal Code* in 2004. The creation of criminal offences, and the punishments prescribed for those offences, reflect Parliament's concern with data integrity, protection and privacy.

The Police Force Regulations

- [28] Regulation 605(1) provides that police officers shall perform and carry out their duties in a proper manner.
- [29] Regulation 607(1)(a) provides that a member of WA Police shall not 'give any person information relating to the Force or other information that has been furnished to, or obtained by, the member in the course of his or her duty as a member ... except in the course of his or her duties as a member'. Similarly, r 607(2) provides that a member shall not, except with the express permission of his or her officer in charge or the Commissioner:
- a. 'use for any purpose, other than for the discharge of his or her official duties as a member, information gained by the member through his or her employment in the Force';
 - b. communicate to the public or to any unauthorised person any matter connected with the Force.
- [30] Regulation 1601 states that a WA Police member who fails to comply with or who contravenes any of the provisions of the Regulations commits an offence against the discipline of the Force. Regulation 601(1) provides that a member shall not act in any manner prejudicial to the discipline of the Force.

- [31] The Regulations further provide for the investigation of offences against the discipline of the Force and prescribe that the offences are disciplinary offences for the purpose of *Police Act* s 23. That section permits the Commissioner, or his appointee, to examine a WA Police member to determine whether they have committed an offence against the discipline of the Force. Various punishments are prescribed for the offence, ranging from a reprimand to dismissal.

WA Police policies on the use of a RACS

- [32] Prior to September 2022, WA Police policy LO-01-06, *Restricted Access to Information on the Police Computer Systems* (LO-01-06) formed part of the Police Manual. It was replaced on 14 September 2022 with LO-01.09, *Restricted Access to Information on the Police Computer Systems* (LO-01.09).
- [33] LO-01.06 provided that:
- a. all access to a WA Police RACS was to be performed in a manner consistent with the WA Police Code of Conduct;
 - b. access was limited to 'business' information which had a direct relationship to the user's work area and access to business information which was not related to a user's work tasks was strictly prohibited;
 - c. access to business information for personal or non-business purposes was strictly prohibited;
 - d. access to a user's personal information or the personal information of their family unless it related to the user's lawful duties and did not constitute a conflict of interest was strictly prohibited;
 - e. users were not to transmit or otherwise share business information with any person except in certain specified circumstances.
- [34] LO-01.06 also contained a note 'to all staff': 'unauthorised access of information ... will be viewed very seriously and may result in management or disciplinary action (which could include loss of confidence or dismissal) or criminal charges'.
- [35] The Police Gazette, 14 November 2018, contained an item on LO-01.06. The item explained that:

Authorisation to use RACS is provided to WA Police Force personnel on the basis of there being a likelihood that access will be required to achieve operational and/or corporate outcomes that are specific to their reason for employment in the WA Police Force.

Authorisation to use RACS does not constitute lawful authority to use RACS to access information when the information is not essential in delivering ... functions of a Police Officer.

- [36] The entry in the Gazette emphasised that WA Police did not authorise the use of a WA Police RACS by a user to access, among other things, information relating to the user's family, extended family, friends or associates or for private or personal reasons.
- [37] LO-01.09 states that 'the access, use and disclosure of RACS is only provided to authorised people required to achieve operational and/or corporate outcomes specific to their employment'. The policy then replicates that part of LO-01.06 which made it clear that unauthorised use of a RACS included use to access information relating to the user's family, friends or associates or information for private or personal reasons. The policy includes an exemption for what would otherwise be prohibited access - where access is deemed essential to the functions of a police officer and the access has been approved by the officer in charge or immediate supervisor (and the approval must be documented).

The Code of Conduct

- [38] The Code of Conduct sets out the expected actions and behaviour of all WA Police employees by reference to the values of duty, teamwork, integrity and care. The Code of Conduct emphasises the need to act lawfully and, among other things, for employees to:
- a. not use their influence, role or position for personal advantage or to the advantage of others with whom they are associated;
 - b. only access, share or disclose agency-held information in the execution of their duty, as authorised by policy or legislation - the Code of Conduct refers to WA Police employees as 'the custodians and protectors of ... official information and records';
 - c. seek advice about the appropriate release of information when unsure.

The underlying policy

- [39] In a digital world, WA Police RACS necessarily hold a vast amount of personal information which is confidential but for its operational relevance. For example, IMS contains an electronic record of incident reports, running sheets and other documents generated during investigations. Access to such information is essential for effective intelligence-based policing and legitimate investigative curiosity is encouraged.

[40] However, the only proper purpose for capturing and storing such information is to facilitate effective policing and much of the information stored in IMS is self-evidently confidential. Consequently, the right to access and use that information is necessarily subject to a proper purpose requirement - that is, a purpose reasonably connected with the functions and duties performed by WA Police officers. The applicable provisions of the *Criminal Code*, the Regulations and WA Police policies give effect to that requirement.

[41] The temptation for police officers to access WA Police RACS for personal reasons is obvious and significant. However, abuses of the right to acquire, store and access personal information undermines public confidence in the integrity of WA Police and risks restrictions being imposed that could impact on operational capacity.

[42] Accordingly, unauthorised access to WA Police RACS and the misuse of electronically stored information by police officers should not be regarded as a trivial matter nor should it be dismissed as a risk inherent in the widespread use of such information for operational purposes. The warning given by the Commissioner of Police on the logon page for IMS is apt:⁴

The information from the system now available to you is confidential and must not be disclosed to unauthorised persons under any circumstances, nor are you authorised to access such information for personal reasons.

Unauthorised access or use of this system and of the information contained within may result in criminal charges and/or disciplinary actions.

Penalty for these offences are severe and may include loss of employment.

[43] There are two further warnings incorporated into IMS.⁵ The need for multiple warnings reflects the importance of complying with the restrictions on the use of a WA Police RACS and the difficulty of detecting unauthorised access. Officer A, in effect, acknowledged the difficulty of detection by accepting that he thought his unauthorised access would 'probably' not be caught.⁶

[44] It is axiomatic that allegations of unauthorised access and misuse of WA Police RACS need to be properly investigated.

Conflicts of interest

[45] WA Police policy AD-84.10 concerns conflicts of interest. The policy defines a conflict of interest as 'any situation in which an employee's financial, non-financial and private interests are directly present and could impact or are

⁴ Exhibit 0027.

⁵ Exhibits 0045 and 0046.

⁶ Officer A, private examination transcript, 26 August 2024, p 74.

impacting upon their public duty'. It further defines 'non-financial' and 'private' interests to encompass any personal relationship that may influence a decision and result in favour or bias for or against any individual or group.

- [46] The policy applies to actual, perceived and potential conflicts. It requires police officers to resolve conflicts in the public interest - that is, in a way that causes no detriment or benefit to any individual or group by a decision, act or omission. It prescribes a procedure for resolving conflicts which, most obviously, includes a requirement that an officer not become involved, or cease being involved, in a conflicted situation.

CHAPTER TWO

The background to the IAU investigation

- [47] Ms M is a friend of Officer A. He has known her for many years and at one time they were in a long-term intimate relationship. He described her in his examination evidence as 'a dear friend ... perhaps the love of my life'.⁷
- [48] Ms M has two children - Ms AM and Mr BM. Ms AM has two children.
- [49] Officer A owns a house in a southern suburb of Perth. He has owned the house since about 2008/2009. Ms AM and her children lived at the house from at least sometime in 2022. In about October 2022, Ms AM's then partner, Mr P, also commenced living at the house.
- [50] The relationship between Ms AM and Mr P ended in August 2023. However, Ms AM and Mr P continued to reside in the house. Officer A moved into the house at about this time and told Mr P to leave.
- [51] In early November 2023, Ms AM obtained a family violence restraining order (FVRO) against Mr P. Subsequently, Officer A contacted police at a southern suburban police station on several occasions to report alleged breaches of the FVRO by Mr P. In doing so, he:
- a. used internal WA Police numbers rather than the public 131 444 number;
 - b. he identified himself to police officers as a member of IAU;
 - c. he sought to discuss matters concerning Ms AM and Mr P;
 - d. in a call to the shift sergeant at the southern suburban Police Station on 4 December 2023, he suggested she access IMS to obtain and relay information to him concerning Mr P. The shift sergeant refused that request and reported the conversation to a superior officer.⁸
- [52] IAU became aware of those matters on about 13 December 2023. IAU conducted an audit of Officer A's access of IMS for the period January 2022 to December 2023.
- [53] As noted above, the audit disclosed that Officer A accessed IMS on 26 October 2022. He conducted a search on the name 'JP' and viewed profile pages for 'JP', 'JWP' and 'JSP'. None of those profiles turned out to be for the former partner of Ms AM.

⁷ Officer A, private examination transcript, 26 August 2024, p 27.

⁸ WA Police Single Officer Internal Investigation Report dated 16 September 2024.

- [54] The IAU audit also disclosed that in October 2022, Officer A had accessed IMS to conduct searches in relation to Mr D. IAU considered that those searches were 'work related'. Mr D had been involved in a traffic incident on 21 October 2022 and Officer A had communicated by email with the supervisor of the police officers investigating the incident.
- [55] The Commission assumes that this finding was made without interviewing Officer A. That is because he accepted in his evidence to the Commission that his access was unauthorised. Mr D was a close friend of Ms M. Officer A was prompted by Ms M to inquire into the incident involving Mr D.
- [56] Officer A was acting in a personal capacity in making those inquiries and in accessing IMS; he had no role in the investigation and was not performing any police function.

The notified allegations and the Commission's Audit

- [57] WA Police's December 2023 notification to the Commission contained two allegations - that Officer A had:
- a. corruptly used his position as a member of the IAU to obtain a benefit in his contacts with police officers at a southern suburban Police Station (the Use of Position Allegation);
 - b. unlawfully accessed a RACS (the Unauthorised Access Allegation).
- [58] The Commission concluded that the Use of Position Allegation had not been substantiated and did not satisfy the requirements for a corrupt use of position to obtain a benefit. The Commission determined that no further action should be taken (CCM Act s 33(1)(d)).
- [59] On 5 March 2024 however, the Commission decided to further investigate the Unauthorised Access Allegation. The Commission's Audit had been conducted by the time the decision was made.
- [60] The Commission's Audit disclosed that:
- a. on 2 September 2019, Officer A accessed the IMS Person Summary for Mr S. Mr S was the then partner of Ms AM and is the father of her children. There is a history of domestic violence involving Mr S and Ms AM;
 - b. on 2 September 2019, Officer A accessed other information concerning Mr S. He also accessed Ms AM's IMS Person Summary;
 - c. on 9 December 2019, Officer A again accessed the IMS Person Summary for Ms AM. He also accessed a police order concerning Ms AM and Mr S, and linked incident reports;

- d. on 18 February 2020, Officer A accessed the IMS Person Summary for Ms M;
- e. on 20 November 2020, Officer A accessed an IMS incident report relating to the non-suspicious death of a neighbour of Ms AM.
- f. on 17 February 2021, Officer A created an entry in the IMS incident report (the 2021 Incident Report) for an alleged stealing incident at an apartment occupied by Ms M;
- g. on 18 and 19 February 2021, Officer A accessed the 2021 Incident Report. He added a running sheet entry to the report on 18 February;
- h. on 1 March 2021, Officer A again accessed the 2021 Incident Report, added a running sheet entry and then wrote off the incident report;
- i. on 24 October 2022, Officer A accessed the IMS Person Summary for Mr D. He also accessed a linked incident report (the 2022 Incident Report) and a running sheet entry relating to the report;
- j. on 26 October 2022, Officer A accessed IMS to search for 'JP';
- k. on 27 October 2022, Officer A accessed the 2022 Incident Report;
- l. on 17 November 2022, Officer A again accessed the IMS Person Summary for Mr D and the 2022 Incident Report. He printed a copy of the running sheet for the report;
- m. on 6 October 2023, Officer A accessed the IMS Person Summary for Mr BM.

[61] Officer A was attached to MAU when he accessed IMS between September 2019 and March 2021. He was the Executive Manager of the Unit in February/March 2021. The remaining instances of access occurred while he was a member of IAU.

The initial WA Police investigation

[62] As noted above, a senior officer within IAU was tasked with investigating Officer A's October 2022 access of IMS. He subsequently recommended that WA Police exercise a discretion not to prosecute a possible breach of *Criminal Code* s 440A.⁹ The reasons given for that decision were:

- a. Officer A's access had not caused any known detriment, there was no evidence he had shared information and he had not accessed sensitive information. Those matters 'significantly [reduced] the perceived seriousness of the offending';

⁹ Review of Exercise of Discretionary Powers to Prosecute dated 2 February 2024.

- b. Officer A was a very experienced officer working in IAU. He was well aware of his obligations around computer access and conflicts of interest and accordingly, he should be held to a higher standard. However, his actions demonstrated poor judgment rather than criminal or corrupt behaviour. Further, 'Officer A's conduct would fall under proposed changes to LO-01.09 (Police Manual - Restricted Access to Information on Police Computer Systems) where it constitutes inappropriate access, as opposed to criminal access - meaning it would be a breach of the Code of Conduct (only)';
- c. his actions were 'likely well intentioned, possibly borne out ... of frustration or a misplaced attempt to assist in a legitimate police intervention, and almost certainly out of a genuine concern for the safety of Ms AM';
- d. Officer A had been a police officer for over 38 years; 'internally, he has no complaint history of similar accesses';
- e. there was a managerial process available which would better address the seriousness of the 'offending'.

[63] The senior officer's recommendations were subsequently approved within IAU and it was decided that a managerial disciplinary process should be followed, with Officer A to be interviewed by another IAU officer as part of that process. There was some delay in arranging the interview but it was eventually fixed for 2 August 2024.¹⁰ However, the interview was cancelled following the decision to reallocate the matter to Major Crime for further investigation.

The further audits of Officer A's access of IMS

[64] The investigation was reallocated after the WA Police Audit. The audit was for the period 1 January 2017 to 1 August 2024 and for possible searches by Officer A on specified individuals and surnames.¹¹

[65] The WA Police Audit disclosed further occasions on which Officer A had accessed IMS and for which no work-related purpose could be immediately identified. Those instances included:¹²

- a. on 13 February 2014, to view records relating to Mr AT;

¹⁰ WA Police Major Crimes division, 16 September 2024 'Internal Investigation Report - Single Officer' in respect of Officer A. Police Complaint Ref IR2023-0467.

¹¹ WA Police Major Crime Division, 20 August 2024 'Review of Exercise of Discretionary Powers to Prosecute' in respect of Officer A. File No: IR2023-0467.

¹² The instances identified in [63] were the subject of allegations considered in the investigator's 'Internal Investigation Report'. There were other instances identified in the 'Review of Exercise of Discretionary Powers to Prosecute Report'.

- b. on 18 December 2014, to view records relating to Ms BT;
- c. on 1 January 2015, to view records relating to Ms CT - Officer A was in a relationship with Ms CT at this time;
- d. on 7 August 2017, to view records relating to Ms YM and Mr BM;
- e. on 30 December 2017, to view records relating to a domestic violence incident report concerning Mr E and Ms DT;
- f. on 17 February 2018, to view records relating to Ms FT and Ms G;
- g. on 7 August 2017, to view records relating to Ms CM and BM;
- h. on 31 March 2018, to view records relating to M and Mr BM;
- i. on 6 December 2018, to view records relating to Ms M;
- j. on 18 February 2020, to view records relating to Ms M;
- k. on 1 January 2023, to view records relating to Mr HT;
- l. on 6 October 2023, to view records relating to Ms M.

[66] On 6 August, Officer A was served with a stand down notice and the investigation was reallocated to Major Crime.

The further reports

[67] The Major Crime investigator produced two reports:

- a. 'Review of Exercise of Discretionary Powers to Prosecute' dated 20 August 2024;
- b. 'Internal Investigation Report - Single Officer' dated 16 September 2024.

[68] The investigator concluded that the exercise of the discretion not to prosecute was appropriate notwithstanding that, in his opinion, there existed a *prima facie* case for establishing a contravention of *Criminal Code* s 440A(3). That conclusion was endorsed by senior officers who reviewed the report.

[69] The Internal Investigation Report identified 20 allegations concerning Officer A's access to a WA Police RACS. The investigator found that:

- a. 17 allegations were sustained;
- b. Officer A should be exonerated on two allegations;

c. one allegation was not sustained.

[70] The investigator recommended that Officer A be given an Assistant Commissioner's warning, and the matter be referred to the IRP. Those recommendations were endorsed by a superior ranking officer.

CHAPTER THREE

Officer A's admissions

- [71] As previously noted, Officer A admitted he accessed IMS on each occasion identified in the Commission's Audit and that his access was unauthorised. Those admissions were volunteered or made without equivocation in response to examination questions.¹³

The circumstances surrounding Officer A's access of IMS

- [72] It is not necessary to detail the circumstances in which Officer A accessed IMS given his admissions, except to note the following.

- [73] In relation to his access of IMS in February and March 2021:
- a. Ms M informed Officer A that there had been a power failure in her apartment due to a fuse being removed. The fuse box was in the underground carpark for her apartment block. She asked Officer A to assist in finding out what had happened;¹⁴
 - b. Officer A spoke to the manager of the corporate body for Ms M's apartment block and obtained access to CCTV film;
 - c. Officer A created an incident report.¹⁵ He reviewed the CCTV film and concluded that the fuse had been mistakenly removed by a Western Power employee. He made entries on a running sheet and then wrote off the incident report. He informed Ms M of the outcome of his investigation;¹⁶
 - d. Officer A did not seek authority from a superior officer to conduct the investigation.

- [74] In relation to the access in October 2022 concerning Mr D:
- a. Mr D was a close friend of Ms M. He was involved in a road rage incident which resulted in a vehicle crash. The incident was investigated by police officers from 'Road Policing Group North' (Traffic Enforcement Division). An incident report and running sheet were created.¹⁷ Officer A accessed those records on IMS. He said he was

¹³ Officer A, private examination transcript, 26 August 2024, p 40 and following; p 73. There were a few instances where Officer A was unable to recall an occasion on which he was alleged to have accessed IMS but he did not dispute what was disclosed by the Commission's Audit.

¹⁴ Officer A, private examination transcript, 26 August 2024, p 50.

¹⁵ Exhibit 0014.

¹⁶ Officer A, private examination transcript, 26 August 2024, pp 51 - 54.

¹⁷ Exhibits 0015 and 0016.

concerned to ensure that evidence of the incident, including any CCTV film, was collected;¹⁸

- b. Officer A contacted a senior sergeant who he had known for many years and who was familiar with the investigation. He recalled speaking to her two or three times about the progress of the investigation;¹⁹
- c. Officer A accepted it was likely that Ms M had asked for his advice about the incident and ensuing investigation. He made his inquiries because of her request.²⁰ He would have communicated something about the result of his inquiries to her but he cannot recall what was disclosed.²¹

[75] Officer A expressly acknowledged he had a conflict of interest at the time that he communicated with officers at the southern suburban Police station about Mr P. The tenor of his evidence was to accept that he also had a conflict when he investigated the fuse incident at Ms M's apartment and communicated with other police officers about the incident involving Mr D.

Officer A's explanations

[76] Officer A explained that his unauthorised access of IMS was motivated in some instances by a concern for the welfare of Ms M and members of her family, particularly Ms AM:

- a. the separation between Ms AM and her former partner, Mr S, had been acrimonious. There were allegations that Mr S had been violent towards Ms AM. Officer A thought it likely he had accessed IMS to ascertain whether he 'needed to have a grave concern for AM's welfare';²²
- b. similarly, Officer A was concerned about the threat he considered Mr P posed to Ms AM. He stated that there were occasions when he refused requests by Ms M for information about Mr P but he 'eventually weakened or got to the point where I was so gravely concerned that that I accessed [IMS]'. He considered Mr P to have engaged in 'pre-

¹⁸ Officer A, private examination transcript, 26 August 2024, pp 58 and 60.

¹⁹ Exhibit 0007 and Officer A, private examination transcript, 26 August 2024, p 58.

²⁰ Officer A, private examination transcript, 26 August 2024, p 58 and 62.

²¹ Officer A, private examination transcript, 26 August 2024, p 63.

²² Officer A, private examination transcript, 26 August 2024, pp 45, 47 and 48. Officer A could not recall accessing IMS in relation to Mr S and accordingly, his explanation was a reconstruction.

homicidal family violence behaviour'.²³ He held similar concerns about Mr S, although not to the same extent.²⁴

[77] Other instances of access were also related to Ms M or members of her family:

- a. on 2 September 2019, in relation to Ms AM;
- b. on 9 December 2019, in relation to Ms AM being listed as a witness to a stealing charge involving water theft at a property where she and Mr S then resided;²⁵
- c. on 18 February 2020, in relation to Ms M;²⁶
- d. on 20 November 2020, in relation to the death of a neighbour of Ms AM.²⁷ He accessed IMS to ascertain whether the death was suspicious;²⁸
- e. on 6 October 2020, in relation to an attempted burglary at a business managed by Mr BM. It was likely he accessed the subject incident report after a discussion with Ms M. He also searched on IMS for similar incidents in the area around Mr M's business premises to see whether they provided evidence from which the offenders could be identified.²⁹

[78] Officer A's access of IMS in connection with the incident involving Mr D, and his subsequent enquiries about the incident, also fell within that category. He stated he was motivated by a desire to assist in the investigation of the incident; that was also his motivation in searching for incidents that may have related to the attempted burglary at Mr M's business premises.

Disclosure

[79] In his examination, Officer A:

- a. could not recall whether he disclosed to Ms M information he had accessed concerning Mr S but 'I may have - I don't know';³⁰

²³ Officer A, private examination transcript, 26 August 2024, p 73. At p 77, Officer A gave examples of Mr P's behaviour, and that of another person, which caused him to fear for the safety of Ms AM.

²⁴ Officer A, private examination transcript, 26 August 2024, p 78.

²⁵ Officer A, private examination transcript, 26 August 2024, p 46

²⁶ Officer A, private examination transcript, 26 August 2024, pp 48 - 49.

²⁷ Officer A, private examination transcript, 26 August 2024, pp 49 - 50.

²⁸ Officer A, private examination transcript, 26 August 2024, p 72.

²⁹ Officer A, private examination transcript, 26 August 2024, pp 68 - 69.

³⁰ Officer A, private examination transcript, 26 August 2024, p 46.

- b. said he did not have a clear recollection but 'I may have told Ms M that there was no ... violent offences [disclosed in the search of IMS concerning Mr P] to try and reassure her that Ms AM was less at risk',³¹
- c. agreed he would have accessed information concerning the attempted burglary at Mr M's business premises after a discussion with Ms M. Again, he had no clear recollection but conceded that he may have disclosed information about the incident to Ms M; although he was not sure, 'I might've said to Ms M that there was another burglary nearby, and that that either did or didn't provide some other investigative actions'.³²

[80] Officer A accepted that his unauthorised access of IMS was prompted by discussions with Ms M or, in the case of the death of her neighbour, Ms AM. He agreed that he had on occasions acted on a request by Ms M.³³ He accepted that it 'might be a fair inference to draw' that he had disclosed information that he had accessed, although 'I can't categorically say that I did or didn't'.³⁴

Officer A's knowledge of WA Police RACS policies

[81] It was clear from his examination evidence that Officer A had a good understanding of the restrictions imposed on access to a WA Police RACS and the reasons for those restrictions.³⁵ He was also well aware of what constituted a conflict of interest and WA Police's policies on the existence and resolution of conflicts. His knowledge of those matters is to be expected given his long experience as a senior police officer and his deployment in IAU.

[82] Officer A was familiar with LO-01.09 and was copied into emails about proposed amendments to the policy.³⁶ He was also familiar with internal WA Police material concerning 'professional curiosity', *Criminal Code* s 440A and the discretion to prosecute alleged contraventions of the section.³⁷ He was involved in at least two investigations into the unauthorised use of a WA Police RACS by police personnel³⁸ and he dealt with the issue in other contexts. For example, he sent an email to a number of police officers in April 2023 reminding them of the risk of contravening s 440A by accessing a particular part of a database maintained by IAU

³¹ Officer A, private examination transcript, 26 August 2024, p 66.

³² Officer A, private examination transcript, 26 August 2024, pp 67 - 68.

³³ Officer A, private examination transcript, 26 August 2024, p 71.

³⁴ Officer A, private examination transcript, 26 August 2024, p 75.

³⁵ For example, Officer A, private examination transcript, 26 August 2024, p 30 and following.

³⁶ Officer A, private examination transcript, 26 August 2024, pp 35 - 36 and exhibit 0022.

³⁷ Officer A, private examination transcript, 26 August 2024, pp 37 - 38 and exhibit 0005.

³⁸ Officer A, private examination transcript, 26 August 2024, p 16.

without a 'legitimate and lawful reason'.³⁹ He understood that 'accessing RACS for private or family reasons, or where a conflict of interest exists, are no-go zones and always will be'.⁴⁰

³⁹ Exhibit 0002; Officer A, private examination transcript, 26 August 2024, p 23.

⁴⁰ Officer A, private examination transcript, 26 August 2024, p 39; the quote is from exhibit 0005.

CHAPTER FOUR

Officer A's unauthorised access

- [83] The Commission found that:
- a. Officer A accessed IMS on the occasions identified in the Commission's Audit;
 - b. Officer A's access on those occasions was not for the purpose of discharging his functions and duties as a police officer but for personal reasons. His access was unauthorised;
 - c. Officer A's access was contrary to restrictions imposed by WA Police policy on access to WA Police RACS. Unauthorised access is a breach of the Code of Conduct;
 - d. Officer A knew that his access was unauthorised at the relevant times.⁴¹

Disclosure of information

- [84] Officer A did not expressly admit disclosing information to Ms M that he had acquired from his unauthorised access of IMS. However, he accepted that it would be 'a fair inference to draw' that he had disclosed accessed information.
- [85] Unauthorised disclosure of information stored on a WA Police RACS is contrary to WA Police policy, the Code of Conduct and the Regulations. It may, in some circumstances, constitute a criminal offence. Accordingly, a finding of unauthorised disclosure is a finding about a serious matter (as is a finding of unauthorised access). The Commission has taken that into account in determining whether it is satisfied that Officer A disclosed information acquired by his unauthorised access of IMS.⁴²
- [86] The Commission was satisfied, on the balance of probabilities, that Officer A did disclose some information to Ms M. The Commission drew that inference notwithstanding that it could not determine precisely what information may have been imparted. However, it is more probable than not that Officer A disclosed accessed information in relation to at least two matters: the missing fuse incident and the investigation into the traffic incident involving Mr D. That is because:

⁴¹ That was an inference drawn from the whole of Officer A's evidence, including his evidence about his knowledge of the applicable policies and admissions he made (for example, Officer A, private examination transcript, 26 August 2024, p 90 - 91).

⁴² See *Briginshaw v Briginshaw* (1938) 60 CLR 336.

- a. Officer A accessed IMS on those matters in response to a request by Ms M;
- b. the request would naturally carry with it an expectation that Officer A would advise Ms M of the outcome of his inquiries having regard to the subject matter;
- c. Officer A's feelings towards Ms M strongly imply that he would have met that expectation by disclosing the results of his inquiries;
- d. it is difficult to envisage how Officer A could have communicated anything about the matters without disclosing information he had acquired from IMS.⁴³

[87] It is quite likely Officer A disclosed information that he had acquired by interrogating IMS about Mr S and Mr P given the concerns that were held for Ms AM's welfare. However, the Commission did not make a finding to that effect. It is conceivable that Officer A was able to advise Ms M about his inquiries in such general terms that accessed information was not disclosed - for example, that he had made inquiries and was monitoring any action being taken by other police officers.

[88] Officer A also accepted that he 'could well have' informed either Ms M or Ms AM about the outcome of inquiry on IMS about the water theft charge.⁴⁴ Again, that is likely given the subject matter of the inquiry. However, there was insufficient evidence about the circumstances in which Officer A accessed IMS on this occasion to enable the Commission to make a finding.

Serious misconduct

[89] The term 'serious misconduct' is defined by the CCM Act to include 'police misconduct'. The term 'police misconduct' is defined to mean misconduct by members of WA Police or 'reviewable police action'. 'Reviewable police action' is defined to include any action taken by a member of WA Police that is taken in the exercise of a power and is taken for an improper purpose'.⁴⁵

[90] The effect of the Commission's findings is that:

- a. Officer A's conduct:

⁴³ In relation to the incident involving Mr D, Officer A stated that, although he had no clear recollection, he 'may well have' informed Ms M of the outcome of the police investigation: Officer A, private examination transcript, 26 August 2024, p 84.

⁴⁴ Officer A, private examination transcript, 26 August 2024, p 87.

⁴⁵ CCM Act, s 3.

- i. breached WA Police policies on access to RACS and disclosure of information;
 - ii. breached the Code of Conduct;
 - iii. contravened r 607(1)(a) of the Regulations (by disclosing accessed information to Ms M);
 - iv. contravened r 605(1) (by not performing and carrying out his duties in a proper manner);
 - v. constituted an offence against the discipline of the Force (r 1601).
- b. Officer A knew that his conduct was in breach of WA Police policies and the Code of Conduct.

[91] In the Commission's opinion:

- a. Officer A's conduct constituted police misconduct within the meaning and for the purposes of the CCM Act;
- b. Officer A exercised a power (the power to access a WA Police RACS) for an improper purpose and accordingly, his conduct constituted 'reviewable police action'.

[92] Consequently, the Commission formed an opinion of serious misconduct.

[93] Officer A's access of IMS was, in some instances, part of a course of conduct in which he communicated with other police officers about investigations in which he had no professional interest. He was in a position of conflict in making those communications. He was also conflicted when he conducted an investigation into the missing fuse at Ms M's apartment block.

[94] That aspect aggravates the seriousness of his conduct. It also highlights an obvious risk with unauthorised access to WA Police RACS - that the offending WA Police officer or employee will seek to become involved in some way in an investigation or other matter in which they have a conflict and which necessarily lies outside the scope of their functions and duties.

The initial investigation by IAU

[95] The investigation into Officer A's access of IMS commenced after IAU was informed of the communication with a sergeant at a southern suburban Police Station. IAU, acting appropriately, identified that Officer A had accessed IMS in relation to the subject matter of his communication. Two decisions were then made. First, to investigate the identified access as a discrete matter and second, that IAU should investigate the matter notwithstanding Officer A's deployment in the unit.

- [96] A more extensive audit of Officer A's access of IMS was not initially undertaken, seemingly as a result of those decisions; the obvious question of whether Officer A had accessed IMS for personal reasons on other occasions was apparently not asked. The extent of Officer A's conduct was only properly identified after the investigation had been reallocated out of IAU. In the Commission's view, the investigation should have been allocated outside IAU immediately as it appeared that Officer A had accessed IMS for an unauthorised purpose. The initial exercise of discretion not to prosecute was endorsed without a full appreciation of Officer A's conduct, as later identified by the Major Crime investigation.
- [97] The Commission notes a further aspect of IAU's dealing with Officer A's unauthorised access of IMS in October 2022. A reason given for exercising the discretion not to prosecute was that his actions were 'likely well intentioned, possibly borne out ... of frustration or a misplaced attempt to assist in a legitimate police intervention, and almost certainly out of a genuine concern for the safety of Ms AM'.
- [98] The human impulse behind Officer A's interrogation of IMS in respect of Mr S and Mr P is obvious. However, it is precisely in those circumstances that WA Police's policies on access are most vulnerable; the policies, the Regulations and the relevant provisions of the *Criminal Code* are intended to apply in the circumstances in which Officer A acted. Concern for the welfare of a family member might explain misconduct by a WA Police officer or employee but it cannot significantly mitigate the seriousness of the conduct.

Conclusion

- [99] For some, the temptation to access RACS without authorisation will always exist. The need to deter, educate and properly investigate breaches is crucial to maintaining public confidence and preventing and combating unauthorised access, disclosure to third parties and corrupt activities.
- [100] The findings in this report demonstrate how easily unauthorised access of RACS can occur. In this case, the conduct was by a senior police officer who maintained a trusted position in IAU, however the lessons can be applied to all public sector agencies utilising RACS.
- [101] Proactive auditing, and promoting an awareness of such auditing, is likely to be effective in assisting to prevent and combat unauthorised access of RACS and potential corrupt activities stemming from such accesses.

- [102] WA Police should give consideration to further defining 'professional and investigative curiosity', in support of existing policies about access to RACS. Access to RACS is either authorised or it is unauthorised and illegal.
- [103] Officer A and the Commissioner of Police were given an opportunity to make representations pursuant to s 86 of the CCM Act prior to the Commission completing its report. They were provided with a draft of this report for that purpose.
- [104] Officer A made no representation.
- [105] In her response, the Acting Commissioner of Police accepted the seriousness of the Officer A's conduct and the need to further educate officers on the WA Police policy on RACS access and use. The WA Police Assistant Commissioner of Standards and Legal has been tasked with a review of the RACS policy and the effectiveness of proactive RACS auditing with IAU. The Commission welcomes that response.
- [106] Pursuant to the CCM Act s 41, the Commission proposes to review the WA Police action taken in response to its review of RACS policy and effectiveness of RACS auditing. The review will consider the steps taken by WA Police to give effect to the issues identified by this report and more broadly, mitigate the serious misconduct risks associated with access to RACS.
- [107] The Commission will conduct its review of WA Police action in 12 months' time.