Corrective Services Administrators' Council

Submission to Parliamentary Joint Committee on Security and Intelligence

Review of the mandatory data retention regime prescribed by Part 5-1A of the Telecommunications (Interception and Access) Act 1979 (Cth)

CSAC Delegates
(Australia)
At 6 March 2020

South Australia	Mr David Brown (Chair) Chief Executive Department for Correctional Services
Australian Capital Territory	Mr Jon Peach Commissioner ACT Corrective Services
New South Wales	Mr Peter Severin Commissioner Corrective Services NSW
Northern Territory	Mr Scott McNairn Commissioner NT Correctional Services
Queensland	Mr Peter Martin Commissioner Queensland Corrective Services
Tasmania	Mr Ian Thomas Director of Prisons Tasmania Prison Service
Victoria	Ms Emma Cassar Commissioner Corrections Victoria
Western Australia	Mr Tony Hassall Commissioner Western Australia Corrective Services Department of Justice

Introduction

The Corrective Services Administrators' Council (CSAC) thanks the Parliamentary Joint Committee on Intelligence and Security (PJCIS) for the opportunity to make a late submission.

The CSAC comprises the heads of Corrective Service agencies in each jurisdiction in Australia and New Zealand. CSAC meet biannually, with working groups progressing Agenda items between meetings. Support is provided by the CSAC Secretariat, which is hosted by NSW.

The primary purposes of CSAC include:

- The sharing of information on current issues and successful initiatives;
- The coordination of cross-jurisdictional work;
- The coordination of responses to national-level initiatives;
- Networking and peer support;
- Agreeing on research topics of mutual benefit;
- Agreeing on protocols for sharing of information and data;
- The coordination of international contributions.

The CSAC provides a valuable forum for Ministers to share information and discuss strategic and national issues. CSAC may approve joint initiatives, provide direction on national issues, and determine shared positions in relation to other groups such as the Council of Attorneys-General.

Mandatory Data Retention Regime Review

CSAC notes the PJCIS is required by Section 187N of the Telecommunications (Interception and Access) Act 1979 (TIA Act) to review the operation of Part 5-1A of the TIA Act (the Mandatory Data Retention Regime (MDRR) Review).

The CSAC notes the PJCIS is able to consider issues and problems that correctional jurisdictions have faced since losing their 'enforcement agency' status following the enactment of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (the 2015 Amendment Act).

The CSAC seeks 'enforcement agency' status for correctional services agencies (CSAs) in Australia so they can detect and prevent criminal activity from taking place within the correctional environment and the broader community, minimise potential terrorist acts being orchestrated from within correctional facilities, and maintain public confidence in their operations.

The lack of access to telecommunications data and information has created obstacles for CSAs in pursuing avenues of investigation, reducing the likelihood of securing a conviction or, in some cases, identifying the likely perpetrator.

Loss of enforcement agency status

Prior to 2015 Amendment Act, any authority or body with functions involving enforcing the criminal law, enforcing a law imposing a pecuniary penalty or a law protecting the public revenue was deemed to be an 'enforcement agency'. These authorities and bodies could authorise access to historical telecommunications data. This enabled CSAs in Australia access to telecommunications data for security purposes.

The 2015 Amendment Act reduced the list of enforcement agencies to a small number of Australian, state and territory law enforcement and anti-corruption agencies. It did so on the presumption that these agencies have, on their face, a "clear operational need and appropriate privacy safeguards".[1]

The 2015 Amendment Act created two forms of enforcement agency status:

1) a general 'enforcement agency' status on a temporary basis under section 176A(3A);
2) a 'criminal law-enforcement agency' status which provides temporary access under section 110A.

Section 176A(3B) is the only mandatory requirement of which the Minister must be satisfied to make a declaration under s 176A. It provides that the Minister must not make the declaration unless the Minister is satisfied on reasonable grounds that the functions of the authority or body include:

(a) enforcement of the criminal law; or

(b) administering a law imposing a pecuniary penalty; or

(c) administering a law relating to the protection of the public revenue.

A number of other factors must also be taken into account by the Minister under section 176A(4) in considering whether to make a declaration, although the Minister need not be satisfied of every such consideration.

Section 176A also imposes an expiry limit of 40 parliamentary sitting days of either House of Parliament, which means agencies would need to seek a declaration on a regular basis. This is an unsatisfactory solution for CSAs, which have an ongoing need to access telecommunications data in order to effectively perform their functions. The process of seeking regular declarations is also time consuming and resource intensive.

Although section 110A(3) of the TIA Act (authority or body can be declared a criminal law-enforcement agency) could provide an alternative basis for granting temporary access to telecommunications data, a legislative amendment to section 110A(1) would be required to include a CSA as a prescribed criminal law-enforcement agency.

Need for 'enforcement agency' status and access to telecommunications data

The CSAC submits that State and Territory CSAs should be given ongoing 'enforcement agency' status under the TIA Act and access to telecommunications data. State and Territory CSAs are an integral part of the Australian law enforcement framework. They have an important role in the detection, investigation and prosecution of serious crime and corruption under State and Commonwealth legislation.

Examples

Corrective Services NSW (CSNSW) is a public agency within the Stronger Communities cluster of the NSW Government. It administers the *Crimes (Administration of Sentences) Act 1999 (NSW)* (CAS Act) and is the primary agency responsible for the enforcement of custodial and non-custodial sentences in NSW. CSNSW undertakes a variety of detection, investigation, and prosecution efforts under both NSW and Commonwealth legislation:

[1] Commonwealth Attorney General's Department, Guide to enforcement agency status.

- *Detect, investigate and prosecute correctional centre offences*

  Part 13A of the CAS Act lists offences relating to places of detention. Offences under this part are investigated, prosecuted, and otherwise administered by CSNSW. Offences vary in nature (apart from their relation to places of detention) and maximum penalties can range up to 50 penalty units ($110 per unit in NSW) or imprisonment for 2 years, or both.

- *Detect, prevent, and assist in the prosecution of various non-correctional centre State-based offences*

  Offences outside the scope of Part 13A of the CAS Act are dealt with by NSW Police with the assistance of CSNSW. Offences in this category include offences relating to escape from lawful custody under the NSW *Crimes Act 1900*;[2] offences relating to the threatening of outside individuals with a mobile phone,[3] and drug offences under the NSW *Drug Misuse and Trafficking Act 1985*.[4]

- *Detect, prevent, and assist in the prosecution of State and Commonwealth-based offences involving acts of terrorism*

  Prior to the 2015 amendment, CSNSW utilised telecommunications data to, among other things, conduct security vetting checks on high risk and national security offenders. This included undertaking subscriber checks to prevent potential terrorist acts being planned or orchestrated from within a correctional facility.

The ability of CSAs in Australia to access telecommunications data is vital to ensuring the safety and security of both the correctional environment and the community.

Example

In Victoria, prisoners have previously utilised telephone communications to make threats towards people in the community and engage in ongoing family violence during their incarceration. The Corrections Victoria (CV) Family Violence Service Reform Strategy is committed to reducing family violence. One of CV's priorities has been to improve identification of perpetrators of family violence. A common condition of family violence related Interim Violence Order (IVOs) is that the perpetrator is prohibited from making contact with people protected by the order. When it is believed that a breach of family violence IVO has occurred using the Prisoner Telephone Service (PTS) telecommunications data is critical in determining the subscriber of a telephone service. For example, CV Intelligence Unit regularly form suspicion or receive information suggesting that prisoners are maintaining PTS contact with adults and children protected by family violence IVOs. Confirmation of this suspicion using telecommunications data would constitute a breach of a current IVO, inform criminal law enforcement agencies and protect community members from further harm of this nature occurring from within CV facilities.

As noted by the Australian Commission for Law Enforcement Integrity, exponential growth in the use of telephony can lead to serious organised crime actors to harness the power of technology to improve their ability to communicate.[5] A common example in the corrections context is the unlawful use of mobile phones. In this regard, mobile phones raise significant security concerns as they can be used to arrange escapes, threaten and intimidate witnesses or victims, traffic contraband, and facilitate communication with offenders outside a correctional centre.[6] In Victoria, seized

[2] *Crimes Act 1900* (NSW) Part 6A.
[3] Acts of this nature can constitute an offence under both State and Commonwealth legislation.
[4] Where the amount is greater than a 'small quantity'. Trafficking of a prohibited drug that constitutes a small quantity is dealt with under Part 13A of the CAS Act.
[5] Australian Commission For Law Enforcement Integrity submission to Parliamentary Joint Committee on Security and Intelligence, 4.
[6] ACT Corrective Services strongly associates itself with this example. Without access to information through the TIA, mobile phones are the gateway through which entry of contraband is facilitated into ACT correctional facilities. Being able to identify evidence and intelligence on such mobile phones

phones have also been found on occasion to reveal evidence of either actual or planned offending behaviour, including child pornography, planned violent activity or terrorist related propaganda or discussion.

Evidence also suggests that multiple prisoners share individual mobile phones, and are able to make a significant number of unmonitored communications each year, presenting a serious threat to correctional facilities and the wider community.

Although CSAs have a range of strategies to detect and prevent inmate mobile phone use, the use of telecommunications data (call charge records and SIM card registration details) following the detection of unauthorised mobile phone use in correctional centres would allow for identification and, if deemed appropriate, prosecution of the inmate or inmates found to be linked to the mobile phone. In this way, criminal associations operating from within correctional centres can be identified and prevented. This has a direct effect on community safety.

Example

Prior to the 2015 amendment, Corrections Victoria (CV) were also able to utilise telecommunications data to determine the identity of, and intercept a person who was planning to traffic contraband into a correctional facility. As an example, prior to the planned incident, a prisoner had used the PTS to coordinate the trafficking with an associate. The associate provided the prisoner with the name and telephone number of a third person. The conversation indicated this person would attend a scheduled visit with another prisoner at the same location and traffic the contraband into the prison over the weekend. CV utilised telecommunications data to find the subscriber details of the telephone number. As suspected, the subscriber details were not the same as those shared by the prisoner using the PTS. CV staff identified the subscriber was a visitor of another prisoner at the location and targeted the individual for a search at their next visit. This person was in possession of a significant contraband quantity. The information required to identify the intending trafficker would not be available without telecommunications data.

In South Australia, the Corrections Intelligence Unit (CIU) previously received information from the cellmate of a suspected drug dealer that the dealer was using two mobile phones to advance his business within the prison. The cellmate provided the service numbers of these phones to CIU staff, who in turn provided these to South Australia Police (SAPOL). Due to differing priorities and backlogs a digital forensic study of these mobiles was not conducted, leaving the CIU with the only option of organising the seizure of the phones. This seizure also provided the SA Department for Correctional Services (DCS) with a major drugs find. However the ability to intercept the numbers provided would have been invaluable in breaking the wider group involved in the trafficking. Currently DCS is reliant on an external agency to complete their investigations.

In the case of community corrections, some high risk offenders (particularly serious sex or violent offenders) have court imposed conditions attached to their release or supervision in the community which prohibit access to certain associates, media, communication methods, devices, or internet services. To enforce these orders, the offender's devices need to be regularly checked to ensure the offender is not engaging in any re-offending behaviour, which may pose a risk to the community. These checks can only be validated through the accessing of call charge records and metadata held by telecommunications providers.

through access to information through TIA, ACT Corrective Services will be able to identify offences and prevent access to contraband such as drugs.

Examples

The NSW inmate population is over 13,000 with approximately 35,000 under community supervision. Offender conduct and associations could result in the identification, apprehension and conviction of a substantial number of people who could pose a threat to the safety and security of correctional centres, members of the community and national security.

In Queensland, there are currently approximately 10,847 Domestic and Family Violence flagged offenders either in custody or being supervised by Queensland Corrective Services (QCS). A significant number of prisoners contravene Domestic and Family Violence orders through illegally maintaining contact with an aggrieved from custody. The ability to confirm the identity linked to mobile and landline telephone numbers would provide the increased capacity to identify these breaches and withdraw this contact, therefore protecting these victims.

In Victoria, CV manages approximately 12,500 offenders in the community, either subject to orders made by courts or the Adult Parole Board. A frequent condition of both Parole Orders and Supervision Orders is that the subject of the order is prohibited from communicating and consorting with specific individuals, or in some cases, entire groups, such as persons identified as Outlaw Motorcycle Gang (OMCG) members, or registered sex offenders. Even with auditing of mobile devices, CV is unable to determine with certainty with whom an offender is having contact. To ensure community safety, telecommunications data is required to confirm the subscriber details of contacted numbers and proactively prevent consorting and organised criminal activities between groups of offenders in the community.

Accessible data has also previously been used to minimise potential terrorist acts being orchestrated or executed from within a correction facility. This is critical to maintaining community safety. However, the lack of 'enforcement agency' status prevents CSAs from identifying contacts of offenders deemed a national security threat or adequately vetting proposed visitors or numbers for prisoner contact. Without this status, offenders can continue to associate and plan terrorist activity whilst in custody, using aliases to avoid their communications being detected.

Examples

There are currently 42 inmates in custody in NSW who have been charged with, or convicted of terrorism related offences.[7] There are also a number of inmates who have not been charged with or convicted of such offences, but who are known to have, or are suspected of having, radicalised or extremist views. When 'Extreme High Risk Restricted' or 'National Security Interest' inmates nominate their telephone contacts, CSNSW can use telecommunications data to confirm the contacts' identities, as well as their criminal histories, relationships, and associations. Undertaking subscriber checks can prevent potential terrorist acts being planned or orchestrated from within a correctional facility.

As at October 2017, Victoria had 78 prisoners accommodated in custodial facilities with a National Security Flag (developed by the Australian-New Zealand Counter-Terrorism Committee). Similar to CSNSW, CV also monitor a further cohort of prisoners deemed to have exhibited at least one indicator that they have been radicalised.

In 2014, CV monitored a PTS call and identified a known terrorist offender's associate in the community was going overseas with some urgency, suspected for a terrorist cause. Further investigation was able to identify the individual. CV Intelligence Unit provided the information to law enforcement agencies and the Australian Federal Police (AFP) intercepted the male attempting to leave the country at Melbourne airport, with terrorist propaganda, including material about beheading, found among his property. Without telecommunications data, CV would have been unable to identify the associate and have him intercepted.

[7] As at May 2019.

In WA, a mobile phone was recovered from a prison that had possibly been used by an individual of counter-terrorism interest. Department of Justice (DoJ) Corrective Services was unable to access data such as call charge data to analyse its use from their own expert perspective, and law enforcement partners were restricted from sharing that raw data with DoJ Corrective Services. Instead, DoJ Corrective Services was reliant upon law enforcement partners to interpret the scenario and provide information about how and when the phone had been used. This situation has the potential to impact on CSAs to anticipate, identify and address potential risks relating to their broader safety and security responsibilities.

CSAs also have a responsibility to maintain public confidence in their operations and those of Government. In this regard, CSAs often have a strong 'internal affairs' function, which *proactively* initiates and manages covert investigations into suspected misconduct by agency personnel. This proactive targeting is often based on sensitive intelligence. A CSAs inability to access and share data lowers its capacity to address issues of corruption or maladministration. It is contrary to public interest to prevent a CSA from investigating and, if necessary, prosecuting such conduct.

Example

In SA, the DCS Office for Correctional Services Review (OCSR) became aware of two Correctional Officers (CO's) who had a close relationship with OMCG members and associates in prison. Examination of Facebook photographs established that one of the two COs was socialising with OMCG members and associates. This CO later resigned after he was arrested by SAPOL and charged with drug related offences. While it was suspected that the other CO was associating with OMCG members and associates it was a difficult to prove. Having access to Call Charge Records (CCR) would assist to provide evidence of an association between the second CO and OMCG members and or associates.

With established, emerging and potential money laundering, and terrorism financing activities and vulnerabilities, it is essential for CSAs to be better informed in regard to how criminals launder, move or conceal illicit funds. Key to this consideration is an acknowledgement that to conceal the proceeds of corruption and bribery, public officials use similar money laundering methods as those used by organised crime groups. This includes the use of corporate vehicles, third parties, professional facilitators, international funds transfers and international trade in services payments.

Although the CSAC is aware of efforts to develop joint investigative arrangements with other law enforcement agencies, these efforts have had limited success because agencies are restricted from sharing data by their own legislation and operational priorities. Agencies are also bound by third-party non-disclosure, secrecy or other agreements/legislation, which prevent the sharing of telecommunications data with CSAs. The lack of immediate access to telecommunications data can also impact risk assessments which may only be relevant to CSAs. Information which is not relevant to partner agencies may also be inadvertently overlooked or dismissed or not addressed due to competing priorities.

Examples

The CSNSW Investigations Branch (IB) investigates allegations of misconduct, corruption or maladministration by CSNSW staff. IB operates under the NSW *Government Sector Employment Act 2013* and Parts 16 and 17 of the CAS Act, and works in conjunction with the NSW Independent Commission Against Corruption (ICAC). These internal investigations often require phone records to be obtained from telecommunication providers to assist in the investigative process. The ICAC is unable to share the telecommunications data it holds despite it being an enforcement agency under the Act.

In Queensland, the Queensland Police Service (QPS) had previously had involvement in examining seized communication devices and subsequent call charge and subscriber checks as relevant to investigate and combat matters such drug introduction and trafficking, threats including domestic violence, escape planning and continued organised criminal activity both within and external to the correctional environment, for example sex trafficking. However, increasingly due to limitation of police resources and changing focus of police investigations, seized contraband such as mobile telephones are not examined by police nor do police undertake follow up intelligence enquires unless there is a direct link to a major or significant investigation. This is exposing QCS to increased safety and security risks within the correctional environment and limiting QCS broader ability to protect and support community safety.

In Victoria, a current staff member is allegedly being groomed by prisoners. It is suspected they are using their work phone to facilitate contact with prisoners, their families and ex-prisoners etc. CV cannot prove anything without the call records. Having access to both their work and personal phone call records would enable this to be investigated at an earlier stage. Instead, information about the conduct continues to be reported but cannot be substantiated.

In WA, during an investigation conducted by DoJ Corrective Services Professional Standards Division (PSD) involved a mobile SIM card located in a prison control room. Investigators did not have the authority to conduct subscriber checks to determine whether a staff member may have brought the SIM card into prison. The matter was referred to WA Police seconded to PSD for investigation. Due to the current legislative limitations, WA Police was unable to share information obtained during their investigation regarding the subscriber and the call charge records relating to the SIM card. PSD was reliant on WA Police preferring charges against a prison officer before PSD had grounds to commence disciplinary action against the officer. The restrictions on PSD having direct access to the subscriber and Call Charge Records information increases the risks of ongoing corruption and security breaches at the prison.

In SA, a prisoner only called one person (his partner) on multiple occasions each day via the Prisoner Telephone System (PTS). The prisoners' use of PTS suddenly stopped. The Corrections Intelligence Unit was sure the prisoner had use of a mobile phone, and that this prisoner would be using the phone to call his partner regularly after hours. The prisoner is a member of an Outlawed Motorcycle Gang (OMCG) and was involved in major crimes. This information was shared with external agencies, who carried out investigations into the use of a mobile phone. However the lack of 'enforcement agency' currently restricts the sharing of any findings with SA Department for Correctional Services, effectively ending its involvement and assistance in the investigation.

Protection of telecommunications information

The CSAC views the protection of personal information, which stem from the retention of telecommunications data by telecommunications providers for extended periods of time, with the utmost importance and priority.

CSAC notes that under Chapter 4, Division 4, section 176(4A) of the TIA Act requires the protection of personal information. Under section 176(3) the protection of personal information under a scheme must:

a) be comparable to the protection provided by the Australian Privacy Principles; and

b) include a mechanism for monitoring the authority's or body's compliance with the scheme; and
c) include a mechanism that enables an individual to seek recourse if his or her personal information is mishandled.

For guidance, information protection principles in each State and Territory, except WA, are comparable to Australian Privacy Principles are set out in the following Table.

Nature of principle	**APP**	**IPP**	**IPP**	**IPP**	**IPP**	**IPP**	**IPP**	**IPP**	**IPP**
		NSW	**ACT**	**VIC**	**SA**	**QLD**	**WA**	**NT**	**TAS**
Management of personal information	1-2	3,6,8	1-2	3, 4, 5, 8	1-10	7-8	N/A	3, 4, 5,6, 10	1-5
Collection of personal information	3-5	1-4	3-5	1-5	1-3	1-3	N/A	1.1 to 1.5, 10.1 & 10.2	1,10
Use or disclosure of personal information	6,8,9	10-12	6, 8	2	7-10	5,9,10, 11	N/A	2.1 to 2.3	2,6,8,9
Direct marketing based on information	7	N/A	7	6	n/a	N/A	N/A	N/A	N/A
Quality of personal information	10	8-9	10	3, 4	3,6	8	N/A	3.1	3
Security standards for retained information	11	5	11	4	4	4	N/A	4.1 to 4.2	4
Access to personal information	12-13	7-8	12-13	6	5	6	N/A	6.1 to 6.7	6

Privacy legislation is enacted in each State and Territory (except WA) to ensure CSAs comply with their privacy obligations and the requirements of section 176A(4A) of the TIA Act. In the case of WA, although it has no state privacy legislation (as of February 2020), the WA Government is committed to introducing new whole-of-government privacy and responsible information sharing legislation for the WA public sector. WA has also enacted complimentary legislation under the *Telecommunications (Interception and Access) Western Australia Act 1996*, which enables inspections of an eligible authority's records to ensure compliance with the Act.

Examples

In NSW, the *Privacy and Personal Information Protection Act 1998*, upholds the 11 Information Privacy Principles (IPPs). The IPPs embody the same principles that make up the Australian Privacy Principles (APPs). A summary of the IPPs is available at https://www.ipc.nsw.gov.au/information-protection-principles-ipps-agencies. This framework is augmented by the *Health Records and Information Privacy Act 2002* and the Privacy Code of Practice (General) 2003, and section 257 of the *Crimes (Administration of Sentences) Act 1999* Act (CAS Act), governing the use and disclosure

of information obtained in connection with the administration of the CAS Act.

In the ACT, the *Information Privacy Act 2014 (ACT)*, upholds the 12 Territory Privacy Principles (TPPs). The TPPs are the same as the Australian Privacy Principles (APPs) with the exception of APP9. However, s23 of the *Information Privacy Act 2014 (ACT)* says that the Commonwealth APPs apply to the acts and practices of the public sector agency (in the ACT) as if the agency were an organisation within the meaning of the Commonwealth Act. A summary of the TPPs is available at https://www.oaic.gov.au/privacy/privacy-in-your-state/privacy-in-the-act/territory-privacy-principles/.

In Queensland, section 341 of the *Corrective Services Act (Qld) 2006* (CS Act) provides strict requirements relating to the use of confidential information accessed by persons performing a function under the act, including offence provisions for the improper disclosure of any confidential information. Further to any other legislative requirements, telephone data is considered confidential information by QCS and managed accordingly under the provisions of the CS Act. QCS is further bound by the requirements of the *Information Privacy Act (Qld) 2009* (IP Act), which are consistent with the Australian Privacy Principles, regarding the collection, storage, use and disclosure of personal information. QCS is considered a law enforcement agency specific to the IP Act.

The Northern Territory has similar provisions and personal information is protected under Information Privacy Principles within the *Norther Territory Information Act (2002).*

In Victoria, CV already collects and holds telecommunications data securely under the relevant Victorian legislation. CV has an obligation for the security and record keeping of information under legislation including the Public Records Act 1973, the Information Privacy Act 2000, the Australian Government Protective Security Policy Framework (PSPF) and the Information Security Management Protocol and Guidelines. The Assistant Commissioner Security and Intelligence is responsible for reviewing CV's protective security policies and procedures, as they relate to ensuring intelligence practice is secure. The CV Intelligence Development Committee (CVIDC) meets annually and discusses protective security policy and oversight of protective security practices as a standing agenda item.

CV's Intelligence Management System, Palantir Centurion (Centurion), is an analytical intelligence repository that supports the needs of intelligence practitioners to capture, control and analyse multi-source data in a secure environment. The platform's secure enclave caters for information security classified at the PROTECTED level (under guidelines in the Protected Security Policy Framework 2018). Information classified above PROTECTED is managed separately from this system. Centurion has restriction capabilities such that information contained in the system can be restricted for viewing by specific subsets of CV staff, based on the user's position and security clearance.

In the ACT, Corrective Services will be able to manage reporting requirements under Chapter 4 of the TIA. This will be done by the Intelligence and Integrity unit using its *iBase* system.

Conclusion

The CSAC submits that there is a demonstrated need to access telecommunications data for the investigation, detection, prevention or prosecution of serious crime. The reinstatement of CSAs as enforcement agencies on an ongoing basis to enable access to telecommunications data will assist to:

- maintain the safety and security of correctional environments in Australia
- ensure the safety of offenders, staff and members of the public
- disrupt offenders from engaging in criminal activities whilst in custody or under a non-custodial order
- ensure national security interests, and
- investigate allegations of internal misconduct, corruption and maladministration to ensure public confidence in the correctional system is maintained.