



AUSTRALIAN
**CRIMINAL
INTELLIGENCE
COMMISSION**

Australian Criminal Intelligence Commission

Submission to Productivity
Commission's Inquiry into Data
Availability and Use

September 2016

Contents

Introduction	3
Overview of the Australian Criminal Intelligence Commission	3
Services	4
Response to Terms of Reference	4
Public sector data sets providing value	4
Australian Cybercrime Online Reporting Network	5
National Police Checking Service	5
Legislative and other impediments to data availability.....	6
The Australian Crime Commission Act 2002	6
Commonwealth, state and territory legislation	6
General.....	7
Suggested legislative reform	7
Other Impediments	8
Existing data sharing initiatives	8
National Criminal Intelligence System (NCIS).....	9
Tracking the effect and value of information products	9
General Observations	9
Standardising collection, sharing and release of data	10
Access to Private Data Sets	11
Confidentialisation and data security.....	11
Conclusion.....	11
Attachment A – Details of ACIC Systems and Services	13

Productivity Commission: Inquiry into Data Availability and Use

Australian Criminal Intelligence Commission (ACIC) Submission

September 2016

Introduction

1. The Australian Criminal Intelligence Commission (ACIC) welcomes the opportunity to make a submission to the Productivity Commission (The Commission) Inquiry into the benefits and costs of options for increasing the availability of and improving the use of public and private sector data by individuals and organisations.
2. This submission provides an overview of the current data and information sharing arrangements that the ACIC provides, is developing or is proposing to develop that are of significant benefit to other law enforcement and government agencies and private sector organisations. It outlines the legislative, technical and cultural restrictions that the ACIC faces in its ability to disclose and acquire data and information to and from other agencies and organisations.
3. This submission is unclassified and may be published in the public domain.

Overview of the Australian Criminal Intelligence Commission

4. On 1 July 2016 the former Australian Crime Commission and CrimTrac merged to form the Australian Criminal Intelligence Commission. The *Australian Crime Commission Act 2002* (Cth) (ACC Act) provides the statutory basis for the ACIC.¹
5. The ACIC's mission is to make Australia safer through improved national capability to connect, discover, understand and respond to current and emerging crime threats and criminal justice issues. The ACIC is also responsible for the management of the National Police Checking Service.
6. The ACIC is part of Australia's cooperative effort to combat serious and organised crime, and works with stakeholders across the nation and around the globe to combat threats that transcend borders. The agency is also responsible for providing national policing information systems and services. ACIC stakeholders include:
 - Commonwealth Government law enforcement, intelligence, national security, border security, national regulators, national service delivery, and national policy development agencies
 - State and territory law enforcement, regulatory bodies and justice departments
 - Private sector such as industry, research bodies and academia, and duly accredited agencies.

¹ From 1 July 2016, the Australian Crime Commission (the ACC) established under section 7 of the *Australian Crime Commission Act 2002* (Cth) (the ACC Act) may also be known as the Australian Criminal Intelligence Commission (the ACIC): subsection 7(1A) of the ACC Act and regulation 3A of the *Australian Crime Commission Regulations 2002* (Cth).

7. The ACIC is underpinned by the ACC Act, and has extensive external oversight and internal governance arrangements, which ensure the agency discharges its obligations under the Act. This includes provisions governing its ability to disclose information.
8. External oversight is provided by the ACIC Board, the Inter-Governmental Committee on the ACC, consisting of Commonwealth, state and territory police ministers, and the Parliamentary Joint Committee on Law Enforcement. The Commonwealth Ombudsman, the Australian Commission for Law Enforcement Integrity and Australian National Audit Office also form part of the external governance framework.
9. As a Commonwealth statutory authority the ACIC also has responsibilities and obligations under the *Public Service Act 1999* and the *Public Governance, Performance and Accountability Act 2013*.
10. The ACIC is part of the Attorney-General's portfolio and reports to the Minister for Justice.

Services

11. The ACIC is responsible for hosting, and developing systems and services that provide data storage and matching capabilities for law enforcement and community safety purposes, including:
 - Australian Cybercrime Online Reporting Network (ACORN)
 - National Police Checking Service (NPCS)
 - National Police Reference System (NPRS)
 - Australian Criminal Intelligence Database (ACID)
 - National Criminal Intelligence System pilot program (NCIS)
 - Biometric matching (for example fingerprints, DNA)
 - National Child Offender System (NCOS)
 - National Firearms Licencing and Registration System (NFLRS), and
 - National Missing Persons and Victim System (NMPVS).

Attachment A provides an overview of each of the listed systems and services.

Response to Terms of Reference

The ACIC provides responses against terms of reference of the Inquiry relevant to its remit and purpose.

Public sector data sets providing value

Identify the characteristics and provide examples of public sector datasets that would provide high value to the public sector, research sector, academics and the community to assist public sector agencies to identify their most valuable data.

12. Data directly contributes to the ACIC's understanding of serious and organised crime, volume crime nationally, and to law enforcement more broadly. The ability to share data, with the right people at the right time is a key contributor to delivering law enforcement and community safety outcomes.

13. The ACIC's Australian Cybercrime Online Reporting Network (ACORN), and National Police Checking Service (NPCS) are examples of how the agency collects from, processes, and discloses data and information to the public and private sectors.

Australian Cybercrime Online Reporting Network

14. The advent of the internet has created new and effective avenues for targeting potential victims. Online fraud poses a substantial threat to the financial and overall wellbeing of Australians. With approximately 12.9 million internet subscribers in Australia,² the internet is one of the principal tools for committing consumer or personal fraud. It provides an efficient means of contacting potential victims and can be a rich source of personal information, as well as a practical way of securing payments. It is therefore no surprise that online fraud has developed considerably over the past twenty years.³
15. ACORN is a joint initiative of Commonwealth, state and territory governments, that enables members of the public to securely report cases of cybercrime. It also provides the public with information to avoid falling victim to increasingly sophisticated cybercrime.
16. ACORN is unique in that it has delivered the sole capability in Australia for automatic referral and triage of cybercrime reports nationwide. This helps develop improved responses to cybercrime. The ACIC prepares intelligence and threat assessments on ACORN data to assist in developing a clearer national picture of cybercrime.
17. ACORN provides value to the public sector as it provides the capability for law enforcement agencies to systematically collect and aggregate intelligence data on cybercrime.
18. The Australian Competition and Consumer Commission (ACCC) noted in its *Report of the ACCC on scams activity 2015* that it was endeavouring to ensure that the data it received from ACORN, combined with its Scamwatch data, informed the "national data set of cybercrime."⁴
19. ACORN data further assists agencies such as the ACCC develop ongoing education and disruption work on cybercrime.
20. As more data is made available and linked between public and private sector bodies and individuals, and the techniques and technology employed by cybercriminals evolves, ACORN provides a mechanism for enhancing national understanding of the scope and cost of cybercrime to the Australian community.

National Police Checking Service

21. The ACIC's National Police Checking Service (NPCS) was developed as a response to the lack of a nationally coordinated process to deliver a National Police History Check (NPHC) on an individual. It provides duly accredited public and private sector bodies with national criminal history information to support their assessment of the suitability of people applying for employment, Australian Citizenship or appointments to positions of trust, such as those working with children, the elderly or other vulnerable groups.
22. Accredited Agencies are able to submit requests for NPHCs based on contract conditions between the agency and the ACIC. The NPCS contract sets out the circumstances where an

²<http://www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/8153.0Main%20Features4December%202015?op=endocument&tabname=Summary&prodno=8153.0&issue=December%202015&num=&view=>

³ Australian Institute of Criminology: The reporting experiences and support needs of victims of online fraud Trends and issues in crime and criminal justice no. 518, August 2016.

⁴ Australian Competition and Consumer Commission: *Report of the ACCC on scams Activity 2015*, p78.

Accredited Agency can make an NPHC application on behalf of itself, or on behalf of another agency (a customer) or an individual. Accredited Agencies include Federal, State and Territory government departments and private Australian corporations. The customers of Accredited Agencies that can lodge applications on behalf of those customers are predominately non-government employers or not for profit organisations.

Legislative and other impediments to data availability

Examine legislation or other impediments that may unnecessarily restrict the availability and linking of data, including where the costs are substantial and consider options to reduce or remove those impediments.

The Australian Crime Commission Act 2002

23. As Australia's national criminal intelligence commission, the ACIC must to be able to share information held by the agency with those parties best placed to assist with the prevention and disruption of serious and organised criminality, whether that be with government partners, international counterparts or private sector stakeholders.
24. A key function of the ACIC, as described in the ACC Act, is to disseminate criminal intelligence and national policing information. Section 59AA provides for the CEO (or delegate) to disclose to government bodies, if the CEO (or delegate) considers the disclosure appropriate and relevant to a permissible purpose.
25. The ability of the ACIC to provide data to private sector bodies is governed by specific provisions under the ACC Act, including the need to list the bodies corporate under the *Australian Crime Commission Regulations 2002* and establish written undertakings with each body corporate before it can make disclosures to them. There are additional legislative requirements where the disclosure involves personal information (as defined under the *Privacy Act 1988 (Cth)*).
26. The existing information disclosure provisions create some difficulties. Any information in the ACIC's possession (including corporate and personnel information) is defined as 'ACC information' regardless of the sensitivity, the original owner, the method through which it was obtained or the classification. This necessarily limits the ability of the agency to disclose. The ACIC is seeking amendments to its disclosure provisions to enable the agency to disclose data more efficiently and effectively, while balancing the need for secrecy and protection of sensitive information held by the agency.
27. The ACIC's ability to collect data from the private sector under voluntary arrangements rather than under the notice to produce provisions of the ACC Act, may rely on the ACIC being able to provide some form of valuable data/intelligence to the private sector. Without this incentive obtaining data on a voluntary basis can be difficult, and is further compounded by the need to enter into complex arrangements under the ACC Act in order to share data/intelligence in the first instance.

Commonwealth, state and territory legislation

28. Inconsistencies between similar Commonwealth, state and territory legislation can result in restrictions in the availability and timeliness and the ability to link data. The United States Government "National Strategy for Information Sharing and Safeguarding" made the

comment that “national security depends on the ability to share the right information, with the right people, at the right time”.⁵ This could equally apply to law enforcement.

29. An example of the inconsistencies in legislation arises in the context of spent convictions legislation. The release of conviction information is governed by a complex legislative and policy framework; all Australian jurisdictions, with the exception of Victoria, have legislation governing the circumstances in which information about a person’s criminal conviction(s) may be used and disclosed. Each of the spent convictions schemes imposes broadly similar rules on what and when convictions may become spent, and on limits on what may be done with the information relating to spent convictions. Each spent conviction scheme also imposes a general prohibition on persons disclosing information concerning convictions which have become spent, including bodies politic. The inconsistency in spent conviction legislation can result in a delay in issuing a NPHC.
30. In exercising powers relating to the disclosure of national criminal history check information, the ACIC must take care to ensure that the circumstances of lawful exemptions from non-disclosure are properly applied.
31. Current state and territory privacy legislation also place restrictions on the ability to access systems, information and data. Each regime is prescriptive in dictating how an intelligence dividend can be shared and with whom. For example, the New South Wales Roads and Maritime Services (RMS) is not able to disclose information to non-NSW agencies. While trans-border disclosure rules are being reviewed, until resolved trans-border disclosures are only considered where an agency either serves a warrant or subpoena, or exercises a statutory demand power (binding on NSW) which compels RMS to disclose the information.

General

32. At present, data that is relevant to law enforcement may be collected under a range of laws, each of which imposes a different access, use and disclosure regime contingent upon issues relating to the manner and primary purpose of collection, and in the case of the ACIC the nature of the data collected and whether it was obtained through the use of its coercive powers. In addition, individual agencies may impose caveats on the use or on-disclosure of some or all of their information reflecting operational or privacy concerns and based on either statutory discretions or common law rights over the information. One effect of these multiple differing regimes is that a criminal intelligence product, for example, becomes a mosaic of information drawn from different data sources and subject to different rules on use and disclosure. This in turn means disclosure of the product has to be subject to rigorous checks to ensure legal obligations and inter-agency undertakings are respected. This slows the pace of information exchange and increases the associated administrative costs.

Suggested legislative reform

33. Consideration should be given to a review of information secrecy and disclosure regimes with a view to reducing the number of different regimes to the essential minimum, so that information obtained under particular legislation would attract a specified grade of protection. This would, of course, be a very complex task involving an attempt to compare

⁵ United States of America Government: *National Strategy for Information Sharing and Safeguarding*, December 2012, p 1.

information protection needs in a wide variety of statutory regimes that have been developed and refined over a long period. The Australian Law Reform Council's Report 112 on Secrecy Laws and Open Government in Australia (2009) addressed some relevant issues but was more focused on the need to avoid unnecessary secrecy rather than the facilitation of intra-governmental sharing of information that is legitimately subject to a secrecy regime.

Other Impediments

34. The view of the Joint Parliamentary Inquiry into the Gathering and Use of Criminal Intelligence in 2013 (and one of the drivers behind the National Criminal Intelligence System (NCIS) program) is that there is not enough sharing of data or data access to fulfil expectations across law enforcement. Despite a clear desire to share data, agencies are still not able to share data in a sufficiently effective way.
35. Policies and procedures for data sharing arrangements were initially designed to support case-by-case consideration of documents or files on individuals known to be of interest. While appropriate for its time, data sharing now enables decision making processes to consider larger quantities of data all at once with multiple systems need to be connected and vast data holdings integrated.
36. As a result a great deal of effort goes into developing Agreements of various sorts to share data/information / intelligence across the various departments, even though the documents are often not legally binding and provide no legal standing should something go wrong. Many government agencies would benefit (in terms of efficiency and clarity) from the use of standard information sharing templates, at least for the APS agencies. Government agencies appear to 'start from scratch' on many occasions with a good deal of time being spent on discussions regarding the language within the proposed agreement.
37. Other key themes that inhibit the ability to access and share data across the law enforcement and the public sector more broadly include:
 - information siloes, which result in the need to search multiple repositories for the same entity
 - aged information technology systems that have not kept pace with advances in technology
 - information and data management efforts are duplicated across multiple systems and agencies
 - reliance on manual processes and informal networks
 - limited interoperability between multiple agencies' information technology systems
 - difficulties in managing extreme quantities and qualities of information.

Existing data sharing initiatives

Provide an update on existing data sharing initiatives in Australia and consider recommendations for improving participation in such initiatives.

38. The former CrimTrac agency, which now forms part of the ACIC, was an initiative between the Commonwealth and state and territory police to deliver technical solutions for national policing information sharing to enhance national law enforcement and community safety. It was responsible for establishing such databases as the National Criminal Investigation DNA

Database and the National Firearms Identification Database. The intent of the merger between the ACC and CrimTrac which established the ACIC, was to deliver greater access and connectivity to criminal data and intelligence, and new capabilities to provide law enforcement with the accurate, up-to-date and complete information they need. One of the key initiatives for the ACIC will be the development of a National Criminal Intelligence System (NCIS).

National Criminal Intelligence System (NCIS)

39. On 30 June 2015, the Australian Government announced \$9.8 million of funding over two years under the *Proceeds of Crime Act 2002* to support NCIS proof of concept program. This program consisted of a partnership between the ACIC and 15 other law enforcement, statutory authorities and government departments.
40. The intent of NCIS is to strengthen the sharing of criminal information and intelligence across law enforcement agencies, and the criminal intelligence community. As well as connecting the existing data holdings and making searching across these highly efficient, NCIS will also offer enhanced analytical and collaboration services. By improving information sharing and system agility, law enforcement agencies will have an enhanced ability to detect and disrupt criminal activity.
41. The ACIC is working with multiple law enforcement agencies to test the concepts and design in real-time operational policing. The NCIS pilot program aims to ultimately inform the delivery of a system that is highly useable and an invaluable asset for Australia's criminal intelligence and information capability. ACIC is currently developing a business case, including costings for a 'full build' of NCIS.

Tracking the effect and value of information products

42. The scope and volume of data that may be collected, analysed and shared across law enforcement and government agencies, and private sector bodies continues to increase. This volume and diversity poses both a policy and a service delivery problem, which may be expressed as 'how can producers of information determine whether their products are effective, adding value and the best allocation of resources to produce the information in the first place?'
43. Without this knowledge policy makers and operational areas within government do not have a great array of indicators for improving their products and making them relevant as feedback typically has been burdensome and not a priority for the user. In turn, this impacts on the cost and future design of information systems to better produce, manage and exchange the right data and information.
44. As information producers, ACIC and AUSTRAC are undertaking a joint project to track the effect and value of information products they provide using Block-Chain technology to create 'smart information products', that would allow the tracking of the outcome of the data and information that the agency provides, history of its use, and user feedback through the life of the information.

General Observations

45. It important to note there have already been numerous initiatives aimed at improved information sharing. Due to constraints within the current data sharing environment,

projects are commonly routed down specific design paths. That is, projects tend towards 'hub and spoke' models centred on a lead agency that collects data from partner agencies under very restrictive bilateral sharing arrangements and then distribute results only for a limited purpose within a single domain of expertise (health, immigration, social services, taxation, policing etc).

46. A networked approach to sharing data could be considered whereby access is provided across different government domains for select purposes. A law enforcement cloud, for example, could therefore comprise one component of a broader interconnected hybrid cloud in which business users and analysts could use analytics platforms to answer a range of requirements with cross-domain data.
47. A tangible deliverable might be an "environment" (in the broadest sense of that word), in which approved users could access data to inform policy development and public service delivery functions.

Standardising collection, sharing and release of data

Examine the options for, and benefits and costs of, standardising the collection, sharing and release of public and private sector data.

48. As a service delivery agency, the ACIC has a responsibility to provide its partners with data, information and intelligence in support of decision-making. In particular there is an increasing need to do so in a timely manner, so that the right people have access to the right information to make the right decisions at the right time.
49. Significant effort is dedicated to the development of memorandums of understanding (MOUs) that facilitate the sharing of data, information and intelligence across various government agencies. To improve efficiency and clarity, many agencies would benefit from the use of standard information sharing templates to avoid duplication, inconsistencies with language and excessive administrative burdens.
50. Currently, multiple MOUs are required between each participating government agency (Commonwealth, state and territory) to enable the sharing of information. Often, a single new piece of information exchange between two agencies will need a separate new MOU. In addition, a small change in the information can require an amendment to an MOU, and need the signatures of multiple government ministers. The process is inefficient and will become (has become) unmanageable, as the sharing of information between Australian Government agencies increases to the point where it becomes routine.
51. Government agencies are investing large amounts of money in ICT solutions to enable data and information sharing. For a comparatively small investment, a single MOU could be an equally important key enabler for initiating information sharing.
52. Consideration could be given by government to share analytic applications and services across government if there were an appropriate platform to do so. This would especially benefit smaller agencies and jurisdictions, who would gain disproportionate analytic capacity beyond their own ICT and recruitment capabilities. In essence, agencies could more easily 'rent' capacity and applications to meet specific or short-term needs. The original purchasing agency would need to be able to manage when they rent out applications, so they can meet their requirements, and others do not simply 'ride for free'.

Access to Private Data Sets

53. Law enforcement agencies often approach commercial vendors individually and purchase copies of data already obtained by another department. One example of this is the Official Airline Guide (OAG) flight schedule data. If the Department of Immigration and Border Protection (DIBP) passes travel data to another agency, they may not be able to pass the OAG data elements due to commercial licence restrictions. Consequently, the receiving agency must also purchase OAG data in order to interpret the travel data correctly. This holds true for numerous other data sets.
54. The total cost of this practice goes beyond the monetary expense of buying the same data multiple times. It also costs government time and resources for each agency to ingest, transform, store and refresh data themselves. Moreover, each agency has to establish their own data validation capabilities, for which they are inevitably under resourced. As a result, data quality suffers, adding to the overall cost to government.
55. Whilst government could release more data to the public and private industry, the same logic must indicate government could save considerable costs by purchasing certain commercial datasets with Whole of Government licences. A platform within governments, advertising an existing purchase of commercial data, making it appropriately available or recording requests to access that data, may be the best way to capture actual data sharing requirements across agencies.

Confidentialisation and data security

Consider the effectiveness and impacts of existing approaches to confidentialisation and data security in facilitating data sharing and linking while protecting privacy.

56. Currently, differences in classification schemes and ICT security requirements across levels of government and the private sector inhibit the ability to share data, be it classified or unclassified and reinforce a culture that is overly cautious in its approach to data and information sharing inconsistencies in security compliance has resulted in a culture of being cautious to data and information sharing. In terms of ICT security, there is no requirement for standardisation across the jurisdictions. An agreed approach to security classification across all levels of government would be of benefit.

Conclusion

57. The ACIC collects and provides data, information and intelligence from various sources, including law enforcement and other government agencies and private sector bodies.
58. The sensitive nature of data, information and intelligence that the ACIC collects and generates, for law enforcement and national security purposes, means that it is unable to lawfully share all of its holdings or products with either other government agencies or the private sector bodies. In cases where there are compelling reasons to share data more broadly across the public and private domain, the following factors should be considered:
 - Greater legislative flexibility and consistency to support data exchange, with consideration given to existing information secrecy and disclosure regimes with a view to reducing the number of different regimes to the essential minimum
 - Establishing common data management standards, processes and protocols

- Pursuing common technical and security architectures for data management and sharing.

Attachment A – Details of ACIC Systems and Services

Australian Cybercrime Online Reporting Network (ACORN)

The ACORN is a joint project between the Australian Criminal Intelligence Commission and the Attorney-General's Department (AGD) and all Australian policing agencies.

ACORN is a national online system that will allow members of the public to easily report instances of cybercrime.

This service enables reporting and referral of cybercrime activity and provision of educational information and advice to help prevent cybercrime. The system will receive reports and supporting information from victims of cybercrime activity and will refer such complaints to the appropriate agency for further attention.

National Police Checking Service (NPCS)

The ACIC in partnership with the Australia's police agencies deliver the National Police Checking Service (NPCS). Controlled access to the NPCS is provided to public and private organisations that undertake a rigorous accreditation process, principally for the purpose of ensuring that persons in positions of trust and/or required to meet legislative requirements are adequately screened for relevant police history.

National Police Reference System (NPRS)

The NPRS system provides Australian police agencies with instant access to comprehensive nation-wide information on persons of interest. This system brokers information between state and territory police services to assist law enforcement around Australia.

NPRS supports the NSS system to provide police history information to assist with relevant records release when undertaking a national police history check.

Note: The NPRS system is only available to police agencies and Approved External Agencies (AEA's) for non-policing law enforcement purposes.

Australian Criminal Intelligence Database (ACID)

ACID is Australia's national criminal intelligence and information system and is mandated under legislation. It includes much of the intelligence the ACIC assembles, as well as the intelligence uploaded by our partners. ACID provides 26 Commonwealth, state and territory law enforcement agencies and other regulatory authorities with the ability to securely share, collate and analyse criminal information and intelligence nationally.

ACID offers analysts and investigators functionality and tools to assist with identifying, analysing and sharing critical pieces of information including new criminal trends, emerging methodologies, links between crime groups and cross border criminal activities.

ACID was first developed in 1984.

National Criminal Intelligence System (NCIS)

The NCIS is the proposed replacement for ACID, which will support a more technologically advanced and efficient response to serious and organised crime and volume crime nationally. On 30 June 2015 the Government endorsed the application for \$9.799 million of funding under the *Proceeds of Crime Act 2002* to support the development of the NCIS through 2015-16 and 2016-17.

It is proposed that the NCIS will enable more effective criminal information and intelligence gathering and sharing between national, state and territory law enforcement and intelligence

partners. At its full capacity, the NCIS will connect existing systems and help develop information and intelligence across the spectrum from volume crime through to serious and organised crime and national security.

Biometric Services

National Automated Fingerprint Identification System (NAFIS)

NAFIS is a finger and palm print database and matching system and is available 24 hours a day, seven days a week to all Australian police agencies and the Department of Immigration and Border Protection. NAFIS enables the fast and reliable identification of persons as well as enabling police partner agencies to solve crimes by quickly and reliably establishing the identity of persons of interest from finger and palm prints left at crime scenes.

Note: NAFIS is only available to Australian police agencies and the Department of Immigration and Border Protection. It will be replaced by the Biometric Identification Services system which will provide facial recognition capability in addition to the existing NAFIS capability.

National Criminal Investigation DNA Database (NCIDD)

The NCIDD provides Australian police with the ability to match DNA profiles. The database provides Australian police and forensic scientists with a powerful intelligence tool that crosses jurisdictional boundaries. It is an online entry web based application designed to view potential links between DNA records both at a jurisdictional and inter-jurisdictional level.

Note: NCIDD database is only available to Police agencies and /or their forensic service provider.

National Child Offender System (NCOS)

The NCOS consists of the Australian National Child Offender Register (ANCOR) and the Managed Person System (MPS). NCOS is designed to enable police to register, case manage and share mandatory information about registered persons as required by legislation. It also enables alerts to be generated when registered persons notify that they are planning to travel interstate or overseas. All Australian police jurisdictions use the register.

Note: The NCOS system is only available to police agencies.

National Firearms Licencing and Registration System (NFLRS)

The NFLRS holds information on past and current firearm licence holders, licensed firearms dealers and registered, lost or stolen firearms. NFLRS allows police agencies to confirm details of a registered owner of a firearm prior to responding to an incident. NFLRS is to be replaced by the Australian Firearm Information Network which will include the existing capability of the NFLRS.

National Missing Person and Victim System (NMPVS)

NMPVS provides police and other law enforcement agencies with the ability to undertake national searches on long-term missing persons, unidentified human remains, and disaster victim identification. This national solution helps police in each state and territory share and match information on missing persons, which had previously been limited by the use of localised systems in each jurisdiction.

The NMPVS is made available to forensic specialists who work with Australian police and New Zealand police. Increasing the number of identifications of long-term missing persons will help provide expedient closure for concerned families. It is estimated that 35,000 people are reported

missing each year in Australia. While over 95 per cent of people are found within a short period of time, there remain approximately 1,600 long-term missing persons.