1. INTRODUCTION

1.1 On 1 July 2016, the Australian Criminal Intelligence Commission (ACIC)[1] was established with the merger of the Australian Crime Commission (ACC) and the CrimTrac Agency. The purpose of this merger was to strengthen Australia's ability to combat the unprecedented national security threat and stop criminals exploiting emerging opportunities and perceived gaps in law enforcement information through utilisation of the collective information and intelligence holdings of Australian law enforcement agencies in support of those agencies' functions.

1.2 The ACIC is uniquely equipped as Australia's national criminal intelligence agency with investigative and information delivery functions. Our role includes reducing serious and organised crime threats of most harm to Australians and the national interest and providing national policing information systems and services.

1.3 To perform our role and achieve our purpose, we work closely with national and international partners to:

- collect, correlate, analyse and disseminate criminal information and intelligence
- maintain a national database of criminal information and intelligence
- provide and maintain national information capabilities and services to support
- policing and law enforcement
- provide strategic criminal intelligence assessments and advice on national
- criminal intelligence priorities
- conduct investigations and intelligence operations into federally relevant criminal
- activity which may include the use of coercive powers such as examinations
- provide nationally coordinated criminal history checks
- support the production of crime and justice research to provide insights into responses to crime in collaboration with the Australian Institute of Criminology

1.4 The ACIC is subject to a robust accountability framework to ensure that it uses its statutory powers set out in the *Australian Crime Commission Act 2002* (Cth) (ACC Act) responsibly, effectively and in accordance with the law.

1.5 The ACIC is not subject to the *Privacy Act 1988* (Privacy Act). The ACIC's exemption from the Privacy Act is long standing and has been subject to a number of reviews[2]. The exemption reflects the need to balance an individual's right to privacy with the public interest in combating organised crime, and the tension between the exercise of the ACIC's unique coercive information-gathering powers and compliance with the Privacy Act. It also recognises the substantial protection currently afforded to sensitive information held by the ACIC including secrecy provisions, legislative restrictions on disclosure of ACIC information, examiner's confidentiality directions imposed by ACIC examiners, and comprehensive external oversight of the ACIC's activities.

1 The Australian Crime Commission is also known as the Australian Criminal Intelligence Commission (ACIC). The *Australian Crime Commission Act 2002* (Cth) and the regulations under that Act set out the legal foundation for the ACC/ACIC, including how the agency may be named as well as the functions, responsibilities and powers of the agency, its Chief Executive Officer, Board, examiners and members of staff. The acronym ACIC is used in this document to refer to the ACC except in terms incorporating the acronym ACC that are defined in that form in the Act.

2 See Part 37 of the ALRC Report 108 *For Your Information: Australian Privacy Laws & Practice* esp. para 37.45.

1.6 Schedule 1 to the Privacy Act contains the Australian Privacy Principles (APPs). The APPs set out the standards, rights and obligations that apply to Commonwealth agencies and private sector organisations in the handling, use and management of personal information.

1.7 This Information Handling Protocol[3] (the Protocol) outlines the ACIC's approach to managing personal information and gives effect to its commitment to act in accordance with the APPs wherever reasonably consistent with the effective performance of its statutory functions.

2. GENERAL PRINCIPLES

2.1 The ACIC holds three distinct categories of information which include personal information:

- criminal information and intelligence;
- national policing information (NPI); and
- administrative information - information relating to staff and other corporate matters.

2.2 The ACIC has internal policies and standard operating procedures that govern the management and security of information in accordance with the Protective Security Policy Framework. This Protocol, together with these internal policies and procedures, outlines the manner in which the ACIC manages personal information and ensures that, to the extent that is reasonably compatible with the effective performance of its functions, it complies with the APPs. To the extent the APPs are not compatible with ACIC functions, the ACIC will deal with personal information in a way that is reasonably necessary for the effective performance of those functions.

2.3 The ACIC has consulted with the OAIC in developing this Protocol.

3. COLLECTION OF PERSONAL INFORMATION

3.1 The ACIC has access to a number of investigative and other lawful tools for the purposes of performing its functions[4]. Personal information collected under these functions includes:

- information contributed to the ACIC's custodianship by, or for the use of, agencies with enforcement-related functions for the purposes of maintaining a national database[5] of criminal information and intelligence and for the purposes of providing systems and services relating to NPI; and
- criminal information and intelligence actively collected (including by the use of coercive powers, where appropriate) under the ACIC's general intelligence function (s7A(a) or for the purposes of operations/investigations authorised by the Board.

3.2 The ACIC may lawfully collect personal information about an individual from that individual or from a third party, and with or without the individual's consent, as part of its investigative and intelligence functions or its NPI functions. The ACIC does not notify an individual on whom it collects personal information for these functions of any of the matters set out in APP 5.

3.3 The ACIC will, if necessary, collect personal information from anonymous sources but the value of such information may be reduced by the lack of a verifiable source.[6] The ACIC will retain unsolicited personal information that has value as criminal information or intelligence.

3 This protocol is released under section 60 of the ACC Act to inform the public about the performance of the ACIC's functions. It does not address information held by the Australian Institute of Criminology which is not governed by the ACC Act.

4 A number of these are available to traditional policing agencies, but a number are not (e.g. ACC Act powers). A number are intrusive and in accordance with relevant legislation require warrants or other authorisations. Consistent with legislative and common law protections, information concerning how these techniques are employed by the ACIC and which ones are used in any particular circumstances, is not publicly released.

5 The ACIC may provide a database service via interconnected facilities between the data holdings of contributing agencies rather than receiving such data into a single database operated by the ACIC.

6 APP2 – Anonymity and pseudonymity.

3.4 The ACIC collects personal information as part of its National Police Checking Service. Accredited bodies collect and provide personal information to the ACIC on behalf of individuals and are authorised to apply for police checks on an applicant's behalf. Accredited bodies are required to deal with the personal information in accordance with the Privacy Act under contractual obligations with the ACIC. The processes by which the ACIC collects information for this purpose are lawful and well publicised and the nature of the processes, such as the consent based provision of personal information by the individual, do not leave room for unfair practices in collecting the information. [7]

3.5 The ACIC also collects personal information as part of the normal communication processes relating to the functions and activities of the agency, and personal information relating to corporate service functions.

4. USE AND DISCLOSURE OF PERSONAL INFORMATION

4.1 The ACIC may use or disclose information where it is permissible to do so under the ACC Act and other applicable legislation.[8]

4.2 ACC information is subject to the information protection provisions of the ACC Act which provide controls on the dissemination of any information in the ACIC's possession or acquired by members of staff in the course of their duties.

4.3 Section 51 of the ACC Act prohibits the ACIC CEO and staff, Board members and examiners, from recording, divulging or communicating to any person any information acquired by reason of, or in the course of, the performance of duties under the ACC Act, except where to do so is for the purposes of a relevant Act[9] or otherwise in connection with the performance of the person's duties under a relevant Act. Section 51 continues to apply even after the ACIC CEO and staff, Board members and examiners may have left the ACIC.

4.4 Breach of this secrecy provision is an offence punishable on conviction by imprisonment for a maximum of two years, a fine not exceeding 120 penalty units, or both.

4.5 The primary mechanism by which the ACIC discloses personal information in its possession to other government agencies (including foreign law enforcement agencies) is in accordance with section 59AA of the ACC Act. Disclosure may occur if the ACIC CEO, or delegate, considers it appropriate, disclosing the information is relevant to a permissible purpose (defined in s 4(1) of the ACC Act), and the disclosure would not be contrary to a Commonwealth, state or territory law.

4.6 The primary mechanism by which the ACIC discloses personal information to private sector bodies is in accordance with section 59AB of the ACC Act. Disclosure may occur if the ACIC CEO or delegate satisfy a number of additional statutory tests from those identified in s 59AA that take into account amongst other things safety of a person and prejudice to fair trial in disclosing information. Private sector bodies must also be prescribed by the regulations and must undertake in writing not to use or disclose that information except for the purpose for which it was shared with it. These provisions include additional statutory protections around disclosure of personal information and places obligations on recipients in receiving that information which, if breached, can lead to criminal charges.

> The Board or the CEO may publish bulletins for the purpose of informing the public about the performance of the ACIC's functions, but must not do so if such disclosure could prejudice the safety or reputation of a person, or prejudice the fair trial of a person if the person has been charged with an offence or such a charge is imminent.[10]

4.7 There are special rules under the ACC Act that apply to the disclosure of information from a nationally coordinated criminal history check. This information may be disclosed to the person to whom it relates and to an accredited body.

---

8 APP6 - Use or disclosure of personal information.

9 According to the ACC Act, the term 'relevant Act' means the ACC Act, a law of a State under which the ACIC performs a duty or function, or exercises a power, in accordance with section 55A of the *ACC Act, the Law Enforcement Integrity Commissioner Act 2006* (Cth) or regulations under that Act, or the *Parliamentary Joint Committee on Law Enforcement Act 2010* (Cth) or regulations under that Act.

10 s60 of the ACC Act.

4.8 The ACIC has internal procedures for disclosure of ACIC information which evaluate compliance with source legislative restrictions as well as the ACC Act requirements and requirements for the handling of classified material under the Commonwealth's Protective Security Policy Frame work.

4.9 In addition to the general legislative restrictions on disclosure identified above, the disclosure of NPI is further restricted, by requiring ACIC Board approval before disclosure is made to a government body that is not prescribed in the ACC Act or Regulations as a recipient of NPI. [11]

5. DATA QUALITY & RETENTION

5.1 The nature of ACIC criminal intelligence is such that the accuracy of the information may be contestable. The ACIC takes reasonable steps to assess the reliability of source and other information in its criminal intelligence products and applies a rating prior to disclosure. However, the ACIC cannot guarantee the accuracy, completeness, relevance or currency of criminal intelligence.[12]

5.2 NPI is collected from a number of prescribed agencies who directly input information (including personal information) into or facilitate access via NPI systems or via automated systems uploads. The contributing agency is responsible for ensuring information can be lawfully provided to the ACIC. The ACIC does not alter, modify, validate or remove the information received from police agencies or prescribed agencies in NPI systems without the express consideration and agreement of the contributing agency.

5.3 Where the ACIC appropriately, in accordance with its powers under the ACC Act, collects bulk datasets in furtherance of its intelligence and investigation functions. The ACIC will only retain such information where it is necessary to do so for the performance of its functions, after being satisfied that, in the circumstances, the level of interference with individuals' rights to privacy (both of entities of interest and entities included in the datasets of no apparent intelligence or investigation interest) is justified by the expected value of intelligence or investigation outcomes to be derived from retaining the dataset.

5.4 Where the ACIC collects personal information from staff members, or from individuals under its National Police Checking Service, the ACIC will take all reasonable steps to ensure that information is accurate, up-to-date and complete.

6. STORAGE AND SECURITY OF PERSONAL INFORMATION

6.1 The ACIC deals with a diverse range of sensitive and classified information as part of its core business and is experienced in ensuring information is appropriately handled and secured. The ACIC has extensive (classified) policies and procedures that govern the security of all ACC information, including personal information. These include policies governing information and records management, information disclosure and information security.

6.2 Information held in/accessed via ACIC systems is protected from loss, unauthorised access, use, modification or disclosure through established data security measures. Data security measures include physical and system access restrictions, password protections, data encryption, and audit trails of user access to systems.

6.3 The ACIC complies with the Protective Security Policy Framework and the Information Security Manual and has an extensive integrity framework that protects the ACIC against misuse of ACC information and mitigates corruption risks that include unauthorised access and disclosure of information held by the ACIC.[13]

11 Section 59AA(1B) of the ACC Act
12 APP10 - Quality of personal information .
13 APP11 - Security of personal information.

7. DESTRUCTION AND DE-IDENTIFICATION OF INFORMATION

7.1 Identifying the threat picture from serious and organised crime involves analysis of information over time and often with a broad collection of information from a range of sources. There is generally a requirement for the ACIC to retain criminal information and intelligence subject to contrary lawful requirements. Retained information provides ongoing references required to support intelligence and also provides a baseline for later review, comparative analysis, and amendment. The ACIC adheres to the requirements of the *Archives Act 1983* (Cth) (Archives Act) and other legislation that prescribes requirements for retention and destruction of information such as the *Telecommunications (Interception and Access) Act 1979* (Cth) and *Surveillance Devices Act 2004* (Cth).

7.2 Any request for correction of data will be referred to the contributing agency for consideration in accordance with their statutory obligations.

8. OVERSIGHT

8.1 The ACIC is subject to a robust accountability framework. Should an individual have a complaint about how the ACIC deals with their personal information, in addition to avenues of access under the FOI Act and depending on the nature of that complaint, the ACIC's conduct can be examined by:

- **the Commonwealth Ombudsman** – who can investigate complaints about the ACIC's actions and decisions to see if they are wrong, unjust, unlawful, discriminatory or just plain unfair;
- **the Integrity Commissioner** – who can investigate allegations of corrupt activity by current and former staff of the ACIC, and
- **the Parliamentary Joint Committee on Law Enforcement** – whose role is to monitor and review the ACIC's performance.