Background

This submission has been prepared according to the following terms of reference:

> *Pursuant to the committee's duties set out in paragraph 7(1) of the Parliamentary Joint Committee on Law Enforcement Act 2010, the committee undertook on 30 May 2012 to inquire into the capacity of the Australian Crime Commission (ACC) and Australian Federal Police (AFP) to gather, use and share criminal intelligence to reduce the threat and impact of serious and organized crime. In that context the committee will consider the:*

(a) Role and objectives of the ACC within the context of the National Security Framework
(b) ACC's collection capability, including resourcing, expertise, powers and criminal intelligence community networks
(c) Adequacy of the ACC's criminal intelligence
(d) Availability and accessability of ACC's criminal intelligence
(e) Interoperability of Australian law enforcement agencies in relation to criminal intelligence holdings

CrimTrac submission

CrimTrac's submission focuses on paragraph (e) – the interoperability of Australian law enforcement agencies in relation to criminal intelligence holdings.

Our submission includes reference to CrimTrac systems, as examples, which are demonstrative of different models of interoperability.

As the major problem facing policing and investigative functions in this globally connected society is how to find the 'value' in the phenomenal amount of information generated, CrimTrac's submission seeks to provide an analysis of interoperability in relation to the concept of value and efficiencies.

CrimTrac's analysis may assist and enhance:

- ongoing developments in the area of information sharing and
- potentially contribute further to outcomes that deliver a reduction in the threat and impact of serious organized crime.

CrimTrac

CrimTrac provides access to information that supports law enforcement agencies through collaborative national information systems and services. Examples of these systems include:

- The National Automated Fingerprint Identification System (NAFIS);
- The National Criminal Investigation DNA Database (NCIDD) and
- The National Police Reference System (NPRS).

The objective of CrimTrac is to enhance Australian policing and law enforcement, through the delivery of high quality information services that meet the needs of the law enforcement community. CrimTrac hosts a number of law enforcement data systems that provide storage and matching capabilities.

CrimTrac's information holdings in essence perform the role of a 'reference library' for policing information. In the policing, law enforcement and national security environments there are a range of different levels and categories of information with a particular focus on three broad categories. These are

- **Reference.** This is the basic detail of a person or object, for example an accurate name, date of birth, gender and address, that enables identification of the individual or object and contains enough ancillary information, such as police history, warrants, warnings, to allow a user to determine an initial action.
- **Intelligence.** This is the combination of credible information with quality analysis. It is a process where information is evaluated and conclusions are drawn, resulting in intelligence.
- **Investigation.** This enables decision makers to combine critical information and intelligence, gleaned from seemingly unrelated sources and incidents, into a holistic assessment of a situation. Such an assessment helps to develop a coordinated course of action, and to plan, execute and monitor the situation.

It is important to highlight that:

- the information, facilitated by CrimTrac, is information collected by police for police
- CrimTrac does not own the information – sovereignty of the information remains with the police
- CrimTrac does not link the information in any way;
- CrimTrac does not provide intelligence to policing and law enforcement agencies, however it may provide information that can have value as intelligence
- CrimTrac does not know the value of the information – the CrimTrac reference information provides opportunistic information – the value of which is fully capitalised (and therefore, known and quantifiable) when linkages are made by the police and law enforcement agencies
- CrimTrac does not amend or correct the data. This can only be completed by the sovereign owner of the data.

What do we mean by interoperability? - Defining Interoperability

To define interoperability in the CrimTrac sense, we may consider the classic approach to interoperability, which references:

a. System/tool;
b. Methodology, and
c. Content/data

It is the submission of CrimTrac that the key divergence in relation to interoperability occurs at (c) whereby two approaches become apparent:

1. the interoperability of systems from a technological and access perspective often using diverse language or codes
2. the interoperability of systems from a technological and access perspective based on a *foundation of common language or codes*

each with differing outcomes in relation to efficiencies and value.

The scope of Concept 1 is restricted in its application resulting from the operation of isolated, independent directories that are limited in their ability to interact with each other in an efficient manner. This is due to the systems possessing their own unique directories and identifiers which are applied to the information and subsequently provisioned to other, often centralised, systems on that basis. In other words, whilst the systems may interact with one another, they may not be speaking the same language at their interface. Interoperability suggests that you can 'talk' and 'share' information, but the value and efficiency of interoperability varies if the information is not consistent or standardised in some way. The absence of standardised codes places a significant burden on users through the amount of time and lost efficiency required to access the required information.

Concept 2 is prefaced on the basis of 'federated directories'. By explanation, federation is the technology and business arrangements necessary for the interconnecting of users, application and systems. Federated directories:

- interact and trust each other
- support consistent business practice
- have a common language or 'directory of codes', that delivers ease of search-ability
- are not dependent on their own capability all the time
- acknowledge and accommodate sovereign ownership (explained below), and
- allow secure information sharing between applications.

CrimTrac proposes that the greater the commonality of language and code, the greater the benefit; and, conversely, the greater the lack of commonality of language and code, the greater the cost of provisioning and consumption of data. Following from this, it is Crimtrac's submission that the measure of success in relation to interoperability is more about the ability to 'retrieve the information that you need to retrieve' in order to utilise criminal intelligence and policing investigative data, rather than value assigned to interoperability through systems' ability to link to other systems (ie 'like' to 'like').

The following discussion of the CrimTrac systems – National Automated Fingerprint Identification System ('NAFIS'), National Criminal Investigation DNA Database ('NCIDD') and National Police Reference System (NPRS) –

complemented by a brief discussion about N-DEx in the United States – may serve to illustrate the above points.

NAFIS

By the 1940s, police in Australia had created a national information capability based on fingerprints using the central fingerprint bureau in New South Wales. The capability of the bureau was extended in 1986 with the introduction of the NAFIS.

NAFIS assists police across Australia to establish identity from fingerprint and palm impressions quickly and reliably and contributes to solving crimes. NAFIS contains fingerprint and palm images as well as basic biographic information obtained from individuals by police agencies. The system also contains unsolved fingerprints and palm print (latent) crime images against which jurisdictions can see new or existing records.

In the case of NAFIS, we use the nationally operated centralised model where data is standardised and there is a nationally uniform application for access and provisioning the data. In this respect, the 'connections' are apparent at the time the request is made by the user.

The NAFIS approach to interoperability is successful, however there has been over 90 years of socialising this conceptual approach, and the data is unexceptional in that it is very regulated, defined and managed. In instances such as the NAFIS and other data sharing requirements with similar data properties to NAFIS, it is likely that the centralised NAFIS model will provide the greatest degree of efficiency and effectiveness and may garner the greatest degree of jurisdictional support.

NCIDD

NCIDD provides the ability to match DNA profiles collected across Australia. For Australian police and forensic scientists this is a powerful investigative tool that crosses jurisdictional boundaries.

NCIDD contains DNA profiles from samples collected by all Australian police services. Profiles may include the case number, jurisdiction, name of officer collecting the sample, name of biologist in charge of the case, type of sample (eg volunteer), name of officer uploading the sample, type of mixture, loci values, action required, match reference, match criteria, comments about the sample, date of match and control information. This DNA evidence is of significant importance to all law enforcement agencies, including the AFP.

In the case of NCIDD, the interoperability model is a varied hybrid model where there is a nationally provided and operated database and matching tool, with most jurisdictions maintaining their own systems on one form or another.

The key to interoperability and national information sharing in NCIDD is the centrally provided profile matching (within CrimTrac) and the subsequent referral to the relevant information owner if there is a match. This approach accommodates the competing needs and benefits of national information sharing in relation to sovereign ownership of the information and local policy considerations (largely around personal and privacy considerations).

NPRS

Police use the NPRS to access a range of operational police reference information, held by other jurisdictions, to assist them in their investigations. The NPRS currently holds 8.7m person records and 2.8m photographs and allows police to access information, for example, about names and aliases, identity details (including photographs), warnings, warrants, etc. The NPRS provides access to vital information for Australian police agencies and Australian Government law enforcement and national security agencies. For example, the AFP and ACC rely on information obtained through NPRS to support their intelligence activities and investigations.

The information provisioned to CrimTrac to deliver the 'reference data' is sourced from the separate and independent systems of policing of the eight federal, state and territory police agencies. This is illustrative of Concept 1. There are impediments in gathering consistent data from disparate systems from a range of sources, and whilst the information is made available to agencies such as the ACC and AFP, the value of this interoperability may be enhanced if we could achieve efficiencies in 'making the connections'.

Investment of time and effort

The current investment of time and effort in relation to interoperability may be illustrated by the following.

Agencies, such as CrimTrac, that facilitate the sharing of reference information, have a potential for a high rate of return/value or, in other words, a low level of effort is required to attain high results. It is usually considerably less expensive to collect information at first contact, when the subject is likely to be present and details are more easily verifiable, than to retrospectively attempt to verify and validate information during an investigation. It should also be noted, however, that without applying due diligence when entering the information and having robust checks for user data entry errors (including the resolution of subject identity issues), the value of the information can be limited. Accurate information has flow on benefits to the user as they do not have to check and potentially amend the material down the track. The greater the accuracy and validity of the identifying and reference information, the higher user confidence will be that the information can be trusted and effectively used for multiple purposes.

Entities that work largely in the intelligence domain could expect that the effort expended roughly equals production of a result. Intelligence is the combination of credible information with quality analysis. It is a process where information is evaluated and conclusions are drawn, potentially creating intelligence.

Police focus on investigations using reference, intelligence, and other information from a range of sources. This enables decision makers to combine critical information and intelligence, gleaned from seemingly unrelated sources and incidents, into a holistic assessment of a situation or matter under inquiry. Such an assessment helps to develop a coordinated course of action, and to plan, execute and monitor the situation. This would generally mean that a high rate of effort is required to produce a result.

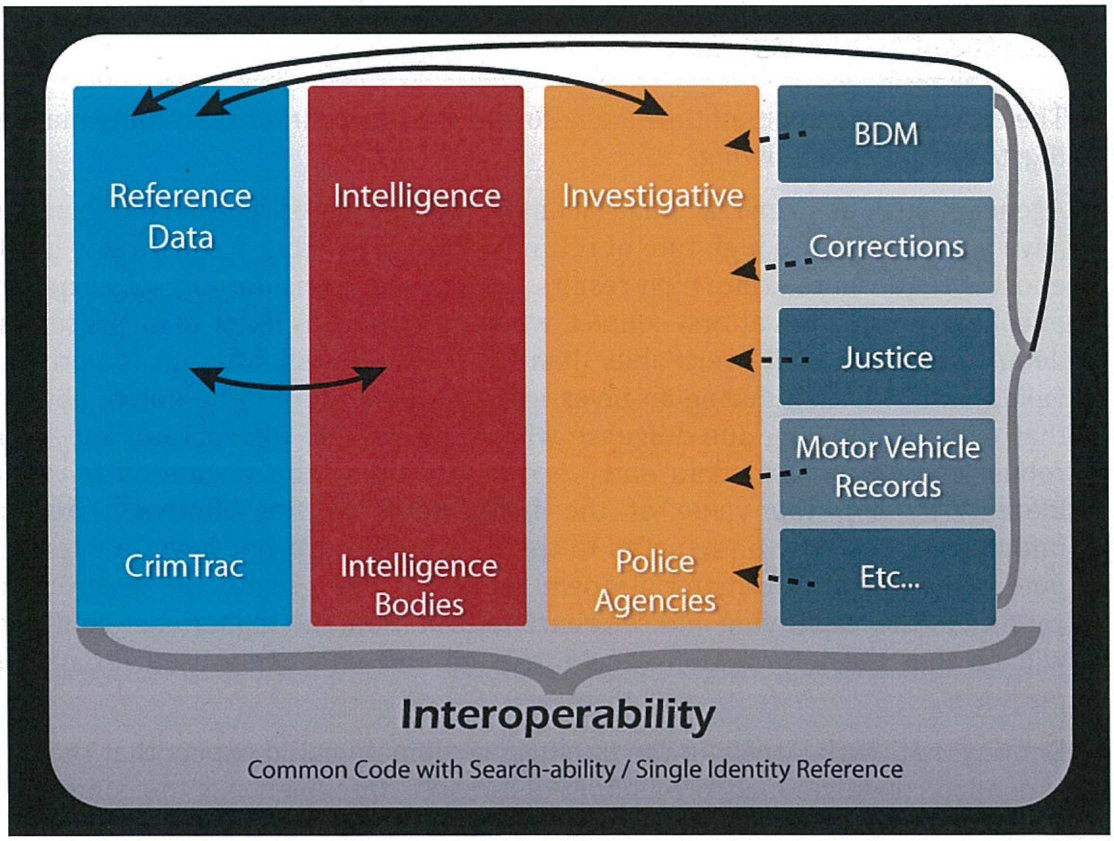
If we apply a 'cost' (time/effort) consideration to this process, it may be identified that funding and labour effort invested at the 'reference' end of the interoperable process, may deliver the greatest return.

If reference data provided by the agencies is

- consistently provisioned
- is linked to a common 'code', and
- provides a search tool operating on the basis of this standardised code directory

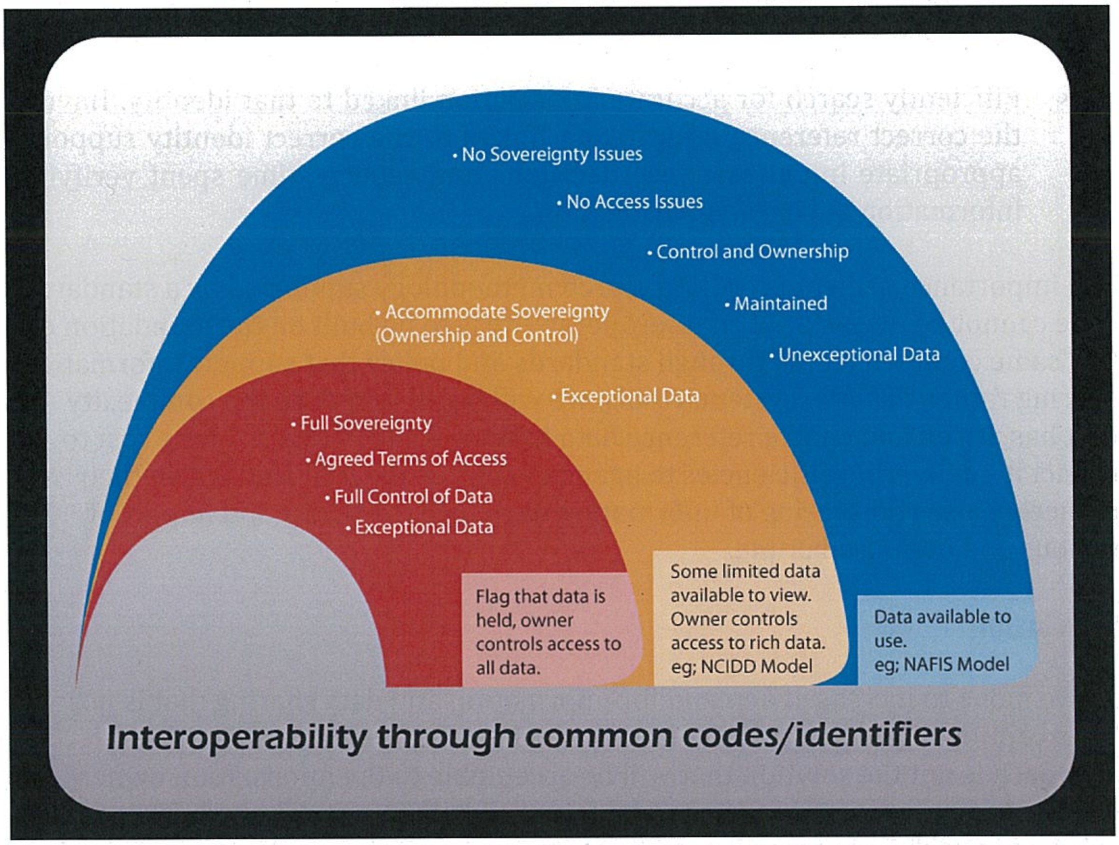
the time, cost and complexity placed on the investigative and intelligence functions may be reduced.

The absence of a standardised code directory that can operate across systems is the dependency upon which the success and absolute value of interoperability hinges.



Sovereign ownership and interoperability

The above discussion is prefaced on the basis that interoperability can be achieved if agencies are able to share their information on the basis of agreed coding arrangements, and yet it also manages to accommodate the implicit tension within the concept of interoperability - that of 'ownership' and control of information ('sovereign ownership').



- No Sovereignty Issues
- No Access Issues
- Control and Ownership
- Maintained
- Unexceptional Data

- Accommodate Sovereignty (Ownership and Control)
- Exceptional Data

- Full Sovereignty
- Agreed Terms of Access
- Full Control of Data
- Exceptional Data

Flag that data is held, owner controls access to all data.

Some limited data available to view. Owner controls access to rich data. eg; NCIDD Model

Data available to use. eg; NAFIS Model

Interoperability through common codes/identifiers

As the above picture seeks to illustrate, the use of standard codes does not impede the agency, from which the data originates, to maintain control of the information as they determine what can be accessed and the uses to which it is put – however, the use of standard codes does not guarantee information sharing *unless* a policy commitment has been agreed.

The US Law Enforcement National Data Exchange (NDex)[1] provides participating agencies with the ability to link information across jurisdictions and 'connect the dots' between apparently unrelated data without causing information overload. This capability occurs primarily in the realm of structured, consistent codes supported by search capabilities, rather than data aggregation to central databases. Ownership and control of the data through N-Dex remains that of the participating agency.

[1] N-DEx is a US criminal justice information sharing system that provides nationwide connectivity to disparate local, state, tribal, and federal systems for the exchange of information

Where could we envisage the greatest value in relation to interoperability?

Underpinning the ongoing value of almost all capabilities for information sharing is a need for robust identity resolution and management. There are two aspects to consider in the provision of a common standard/code for identity; the ability to:

- Correctly identify the individual, or object, thereby reducing time spent searching for the correct record and eliminating false positives, (where the amount of time spent resolving ownership issues could be the greatest cost)

- Efficiently search for accurate information linked to that identity. Having the correct reference information linked to the correct identity supports appropriate initial response decisions and reduces time spent verifying information during an investigation.

The importance of an appropriate search methodology supported by a standard code cannot be over-stated. If interoperability is to be built on the foundation of the 'same common truth', through standards and policy that support information sharing rather than the systems/tools, we will begin to reduce the complexity that has arisen and enable reference data to have value in excess of the cost to collect it - delivering efficiencies to agencies such as the AFP and ACC in their gathering, use and sharing of information to reduce the threat and impact of serious and organised crime.

Conclusion

As we move to increased demand for information and data sharing that is not 'unexceptional' (such as NAFIS), it is increasingly likely that a centralised approach is not the solution that will be acceptable to the information owners. A distributed or federated access model is more likely to suit the need. The solution in each instance will need to be decided on its merits by the information owners.

Conceptually there is little difference in the challenges faced by law enforcement agencies of today and those of the 19th century in relation to interoperability and the sharing of information– for example, the interoperability of communications in the 19th century was made possible by agreed policy and standards (eg: morse code) that delivered efficiencies in information sharing, not the tool/technology alone. In this light, the starting point to enhance interoperability and deliver efficiencies in information resides in a decision concerning agreed standards and policy that support information sharing. The demand for efficient and effective information sharing, and the outcomes interoperability can deliver may not be fully realised without such a 'back to basics' approach.