Information Sharing Approach For the Criminal Justice System

Executive Summary

Final

Not Protectively Marked

Intended Audience, Purpose and Background

The intended audience for this paper are business and IT leaders within the Criminal Justice System (CJS) who, in support of their operational duties and their commitments to the Office of Criminal Justice Reform Programme, have a requirement to share information within and beyond the CJS[1].

The paper is also intended for business and IT leaders across the Public Sector with a similar requirement as the approach defined is designed to be applicable across the sector.

The circulation list for this paper is the CJS Architecture Management Board (AMB) and the Technology Delivery Board (TDB).

The purpose of the paper is to define in summary the common approach for information sharing across the CJS.

While it is enabled by IT the approach defined in this executive summary sets out the *principles* for making information sharing workable across the CJS.

Approval for the paper is sought from the AMB and the TDB in the first instance, before final approval is sought from the Operational Board (OB).

Approval from TDB is sought at the March meeting to be held March 16th 2006.

Once the paper has been approved by the OB, TDB members will be asked to circulate appropriately within their own organisations. Once approved, the paper will also be circulated to the attendees of the cross-Criminal Justice Organisation (CJO) event of October 2005, which was held to define the CJS wide approach to Information Sharing.

The background leading up to this paper is the work of the Office for Criminal Justice Reform (OCJR) focusing on 'joining up justice' and the cross-CJO event of October 2005 held to define the CJS wide approach to Information Sharing.

This paper provides the Executive Summary for the detailed paper produced as a result of this event. The detailed paper is titled 'CJS IT Programme Data Sharing Principles' – draft version 0.4, 27th February 2006.

The detailed paper has been circulated to the attendees of the event and comments have been included. In combination with this Executive Summary approval for the detailed paper will be sought via the AMB, the TDB and then the OB.

[1] Information Management, Information Assurance and Enterprise Architecture professionals within CJOs are requested to review the principles set out in the detailed paper 'CJS IT Programme Data Sharing Principles' and advise their management accordingly.

Document Control

Document Reference

Signatories/Approvers

Level	Name	Date
Architecture Management Board	Carl Bate (Chair)	14/03/06
Technology Delivery Board	John Suffolk (Chair)	11/04/06
Office of Criminal Justice Reform Operations Board	Ursula Brennan	14/06/06

Revision History

Version Number	Author(s)	Date	Summary of Changes
0.3 Draft	Carl Bate, Interim CTO, CJIT Nigel Green, Exchange Strategic Architecture Lead	07/03/06	Comments from CJIT: Directors Ian Hardy, Information Management Lead Enterprise Design Authority Gill Woolfson, Assistant Director, Technology Directorate
0.4 Draft	Carl Bate	11/04/06	Comments from Claire Hamon
1.0 final	Sam Koomson	12/07/06	Final version after approval from OCJR Ops Board 14/06/06

Circulation List

Purpose	Name	Title	Section(s)	Purpose Complete
Approval	CJIT Directors			
Approval	CJIT Technology Directorate			
Approval	AMB			
Approval	OCJR Operations Board			

For further information please contact
Email: sam.koomson@cjit.gsi.gov.uk
Telephone: 020 7035 8085

Contents

1. The 5 Golden Principles

The 5 Golden Principles define what each CJO needs to sign-up to in order to make Information Sharing a reality across the CJS.

The 5 Golden Principles are:

- All agree to a common approach for information sharing
- All agree to federated working which involves adopting a combination of mandated standards for business information interchange which apply to all, and specific standards supporting discrete 'Communities of Interest' for information sharing (such as Charging, Victim and Witness Care and Youth Offender Management).
- All agree to use of the Exchange, the Shared Service to the CJS which provides IT services to enable Information Sharing in an efficient and effective manner
- All agree to treat information sharing as a business imperative enabled by IT, rather than as an 'IT issue only'
- All acknowledge that information sharing can only happen by design, not accident, and that associated investment is required by all for the benefit of each CJO and the CJS. Therefore, within the context of each CJO's business and financial constraints, all agree to invest in Information Management, Information Assurance and Enterprise Architecture capability, intrinsic to supporting the common approach for information sharing

This paper describes the Information Sharing Approach in summary. This paper is the Executive Summary for the detailed paper - 'CJS IT Programme Data Sharing Principles' – draft version 0.4 dated 27th February 2006.

2. Context

Within the National Criminal Justice Board's (NCJB's) vision for the Criminal Justice System (CJS) outlined in its Strategic Plan, CJS organisations when sharing data commit to:

'The proper, secure and consistent sharing of information to support the delivery of an efficient and effective Criminal Justice System'

This paper provides an Executive Summary of the approach for delivering on this commitment.

While it is enabled by IT the approach defined in this executive summary sets out the *principles* for making information sharing workable across the CJS.

In addition, the 'Transformational Government – Enabled by Technology' strategy paper of November 2005 defines the vision for Citizen and Business Centred Shared Services, Delivered Professionally. Within this strategy it is stated that:

'Data [information] sharing is integral to transforming services and reducing administrative burdens on citizens and businesses. But privacy rights and public trust must be retained.'

The approach is also offered as applicable to information sharing across the Public Sector, as well as information sharing *within* Public Sector Organisations, in support of the Transformational Government Strategy.

This Executive Summary is based on:

- *a 2 day cross-CJO (Criminal Justice Organisation) event held in October 2005*; to specifically address information sharing and the detailed paper produced as a result of this event - 'CJS IT Programme Data Sharing Principles' – draft version 0.4 27th February 2006

- *cross-Criminal Justice Organisation on-going work to address information sharing;* including the work of the CJS Exchange (CJSE) Data Standards Forum

- *the 'Information Sharing Shared Service' for the CJS provided by CJIT through the CJS Exchange, and the CJS Exchange Reference Architecture;* which is based on proven, industry leading IT and practices for information sharing across federated organisations and which is also being positioned with the Cabinet Office as the Shared Service to support information sharing across the Public Sector.

Information Management, Information Assurance and Enterprise Architecture professionals within CJOs are requested to review the principles set out in the detailed paper 'CJS IT Programme Data Sharing Principles' and advise their management accordingly.

3. The Core Concept of Federated Working

An efficient and effective end to end justice system requires Criminal Justice Organisations (CJOs) to focus on delivering their specific business operations *and* to work together in a joined up fashion, hence the commitment to efficient and effective information sharing.

This requires that individual CJOs retain ownership of who can access their information and for what purposes. But it also requires a common approach to Information Sharing – i.e. a set of common principles - to be adopted across the CJS.

The CJS Exchange is a key enabler to information sharing as it prevents islands of information sharing being created (which will become a barrier to cross-CJS information sharing) and provides a set of shared business functionality, IT assets and supplier commercial arrangements which delivers economies.

To make use of this Shared Service an agreement is required on a common way of defining what business information is to be shared, who can access it and with what assurance (such as security and legal compliance).

Use of a Shared Service and a common approach to information sharing does not require a single (centralised) controlling organisation to define what information is to be shared and how it is to be shared. The CJOs are a federation of organisations and therefore the Shared Service and common approach have been constructed to support this federated operating model.

Federated working requires:

- Agreement by all parties on a common 'operating model' for information sharing; the common operating model is presented in this Executive Summary
- Agreement by all parties to adopt mandated standards for business information interchange, *both* those which apply to all CJOs and those which are agreed specifically between CJOs; mandated standards which apply to all include the CJSE Data Standards and the e-Government Interoperability Framework (e-GIF) Standards
- The core concept of 'Communities of Interest' to be adopted

The CJS (via the CJSE Data Standards Forum) and e-Government have already defined a set of common data standards which are critical to aid the interchange of business information. However, specific communities will need to adopt these standards and further develop their own to efficiently meet their specific information sharing needs. These needs are not just CJO to CJO at the top-level of the organisations. For example, communities of interest might include:

- Public Servants working on Charging across the Police and CPS;
- Public Servants working on Victim and Witness Care across the Police, CPS, DCA and Prisons and Probation;
- Public Servants working to meet Youth Offender Management needs across the Police, CPS, DCA, and the Youth Offending Teams – which themselves include Public Servants outside of the CJS for example in Health and Social Services

The Information Sharing approach proposes how such communities of interest can work together to agree and govern their information sharing needs enabled by CJIT and the Exchange, while adopting mandated data standards for business information interchange.

4. Information Sharing Approach Foundations

The Information Sharing Approach is founded upon:

- **a core principle of a federated approach and communities of interest;** empowering CJOs to work together on the Information Sharing needs important to them and retain ownership of who can access their information and for what purposes, while adopting mandated interchange standards applicable to all

- **an agreed operating model for Information Sharing;** defining how CJOs work together in an efficient and effective manner to make and maintain agreements on how information is shared based on straightforward concepts and principles

- **business interchange standards;** within the agreed operating model for Information Sharing, data standards relating to information such as personal details, case details, identification and authentication, roles and organisation unit codes which enable information held by one CJO (or government department) to be usable in an efficient and effective manner by one or more other CJOs (or other government departments); note that these standards are based on a hierarchy of mandatory standards, specifically the CJSE Data Standards and e-GIF

- **the existing and planned Information Sharing Shared Service of CJIT and the Exchange;** which enables efficient and effective Information Sharing across the CJS (and which is being positioned as the Information Sharing Shared Service for the Public Sector in support of the Transformational Government Strategy); the Exchange includes services for publishing, searching and viewing information, creating new functionality to use this information (for example Web 'portals'), IT system to system integration which supports creating new functionality in existing or planned line of business systems (for example case file interchange), and information subscription and notification services for Public Servants and IT systems (for example informing a Public Servant when an offender is released from Prison).

- **the Exchange Reference Architecture[2];** the Reference Architecture for Information Sharing across the CJS (and which is being proposed through the CTO Council as Reference Architecture for Information Sharing for the Public Sector in support of the Transformational Government Strategy)

- **existing and planned IT assets within Criminal Justice Organisations and other government departments**; for example information sources and strategic applications which enable business processes within CJOs

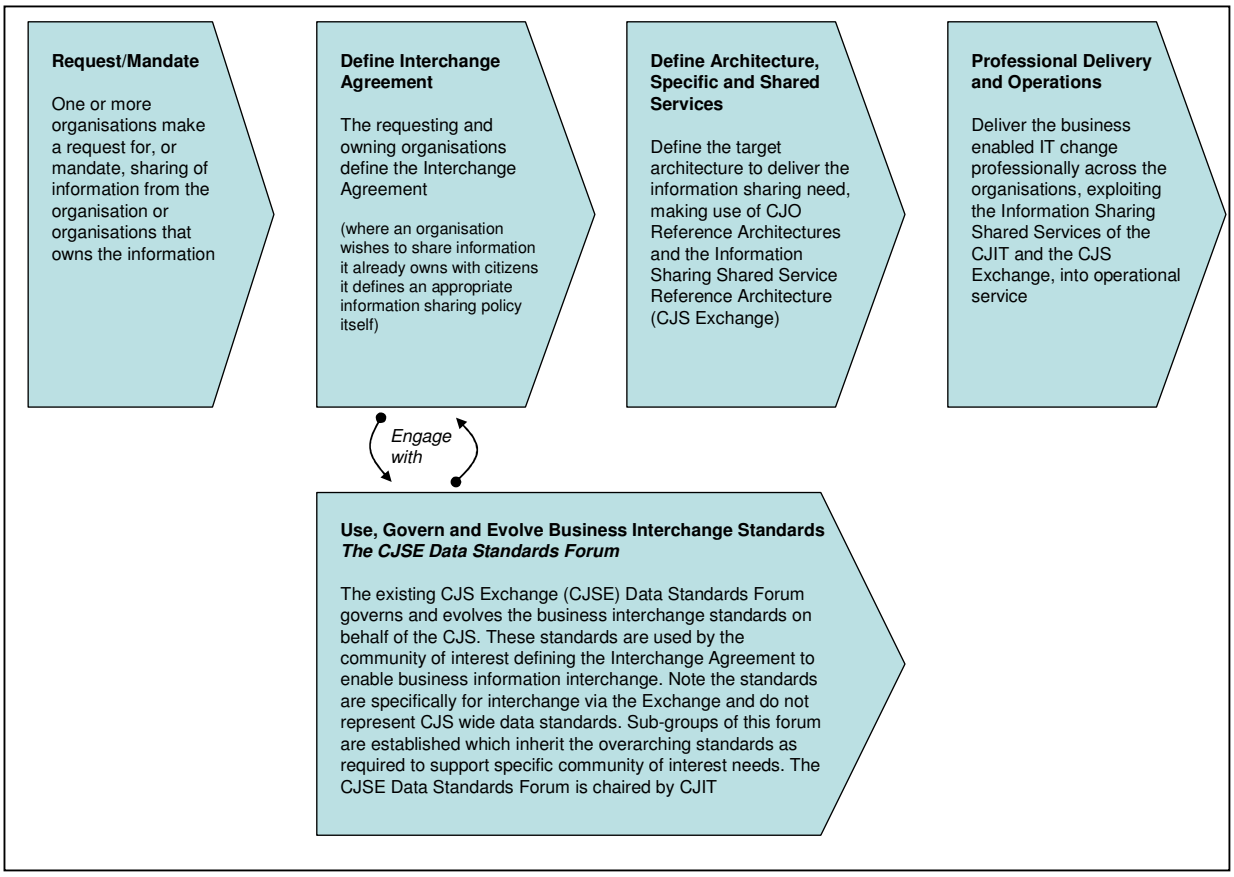
- **technology of the Exchange Shared Service to aid acceleration of Information Sharing;** including 'meta-data' modelling and data access capability which supports analysis of and access to existing information sources within CJOs which currently have different information standards – for example being able to quickly access information relating to a Citizen which is currently stored in multiple different sources in different data formats

[2] The Exchange Strategic Architecture published in November 2005 defines the Reference Architecture for Information Sharing (CJS IT Programme – Contextual, Conceptual & Logical Architecture)

5. Proposed Operating Model for Information Sharing

At the top-level the proposed Operating Model (top-level process) for Information Sharing is shown below. An explanation of core concepts and a scenario to illustrate the Operating Model in action then follows.

Please note that this Operating Model sits along side all existing processes for scoping, approving and delivering business enabled IT change.



The proposed operating model is supported by the following forums and boards:

- The CJSE Data Standards Forum (and specialist sub-groups supporting specific communities of interest) – this forum and CJSE Data Standards already exist
- The CJS Data Sharing Forum (planned to commence from March 2006 to support Data Protection and other legal compliance needs)
- The CJS Information Security Forum (planned to be re-launched)
- The CJS Architecture Management Board (already exists)
- The CJS Technology Delivery Board (already exists)

It is proposed that the CJSE Data Standards Forum, CJS Data Sharing Forum and the CJS Information Security Forum become sub-groups of the CJS Architecture Management Board. The

Architecture Management Board is chaired by CJIT and is a sub-group of the CJS Technology Delivery Board.

It is acknowledged that for some Information Sharing Policies there may be many Information Owners involved.

The CJS Data Sharing Forum will define and share leading practices and IT enabling support to increase the efficiency of the management of such policies.

The key consequence of this operating model (outside of the obvious investment needed to deliver IT enabled business change) is that CJOs will be required to invest business and IT resource in establishing and governing Interchange Agreements and Data Standards for business information interchange.

This will require CJOs to maintain or increase investment in Information Management, Information Assurance (Security) and Enterprise Architecture capabilities. Such investment will vary by CJO and is intrinsic to delivering on the commitment all CJOs have made; 'The proper, secure and consistent sharing of information to support the delivery of an efficient and effective Criminal Justice System'

The core concepts and terminology of the top-level operating model are as follows:

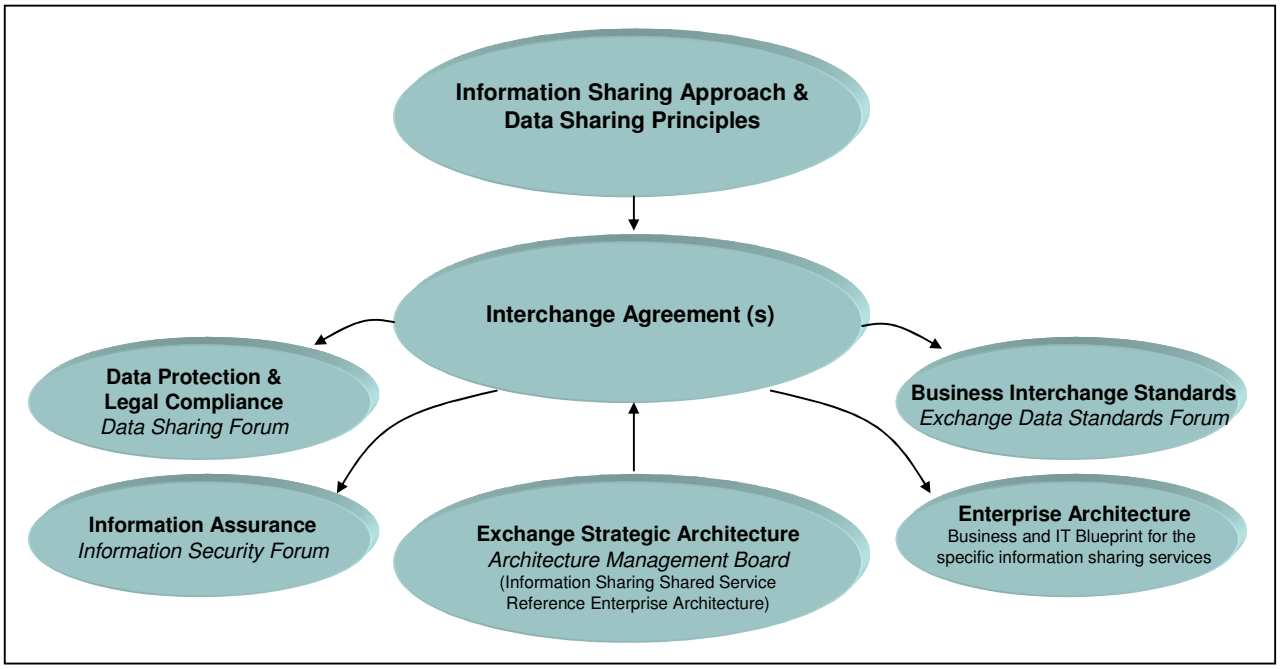
Information	Any data held by or derived by (and therefore also held by) an IT system – be it for the purpose of a one-off task or for the purpose of permanent storage. For example, this includes data (a date of birth), information (age derived from date of birth at a given point in time) and intelligence (how age may affect an individual's behaviour)[3].
Organisation	A body which uses Information. For example, this may be a barrister recognised as a sole trader, a Criminal Justice Organisation recognised as a Public Authority or the Home Office also recognised as a Public Authority.
Information Owner	An Organisation legally recognised as the owner of specific Information and which is responsible for complying with all relevant legislation, including but not limited to the Data Protection Act (DPA) 1998 where the Information Owner is defined as the Data Controller. Information Ownership changes as information is shared – for example: a) if information is moved from one organisation to another, the receiving organisation becomes the owner for the information b) if information is replicated from one organisation to another (e.g. case information is provided by one police force to another, but the first force also retains the case information for its own purposes), the receiving organisation takes ownership of its replicate and the originating organisation retains ownership of the original (its replicate) c) if information is viewed by an organisation, any information retained or inferred after viewing, is owned by that organisation
Interchange Agreement	An agreement made between the Information Owner and one or more other Organisations which defines the policy for information sharing between the Organisations for a specific purpose. This agreement also includes information sharing with citizens. The Interchange Agreement includes the definition of:

[3] The detailed paper from the 2-day event describes the approach to paper information.

	• *Purpose* – defining the community of interest • *What* – what information is to be shared • *Who* – who can access the information, for example a citizen or group of citizens, an individual within an organisation, or a group of individuals undertaking a specific role within an organisation such as 'intelligence' • *Trust Policy* – who the Information Owner trusts to undertake Identification and Authentication (ID&A) for individuals accessing the information, for example whether this is the accessing organisation of the Information Owner itself • *When* – when the information can be accessed, for example as a one-off access only or indefinitely • *How* – how the information can be accessed, for example via a restricted network or a confidential network, and by what type of device (for example fixed or mobile) • *Service Levels* – defining the confidentiality, integrity, availability and other non-functional principles (such as performance and volumes) that relate to the information being published, subscribed to and accessed • *Governance* – the process for managing the Interchange Agreement itself, for example how changes to the agreement can be made and what audit information is required by whom • *CJSE Data Standards Forum Sub-Group* – which (if any) sub-group is required to define the specific interchange standards in support of the Interchange Agreement – inheriting the mandated standards of the CJSE Data Standards Forum and e-GIF.
CJSE Data Standards Forum **&** **Business Interchange Standards**	The defining and governing body of data standards for the information interchange via the Exchange, incorporating CJS wide-standards and specific community of interest standards for business information interchange. These standards include: • *Purpose* – defining the community of interest • *Relationship and Hierarchy* – Business Interchange Standards which are inherited (i.e. the CJSE Data Standards and e-GIF) and any relationships with other Business Interchange Standards • *Business Standards* – the standards which define the information to be interchanged in business terms, for example name, address, case reference, public servant ID • *Implementation Standards* – the standards which implement the business need, for example expressed via XML, RDF and OWL The technology of the Exchange Shared Service can accelerate Information Sharing through 'meta-data' modelling and data access capability which supports analysis of and access to existing information sources within CJOs which currently have different information standards – for example being able to quickly access information relating to a Citizen which is currently stored in multiple different sources in different data formats.

The operating model creates the following relationship between policies:

Please note that these relationships between policies sit along side all existing processes for scoping, approving and delivering business enabled IT change.



The operating model is designed to support the full range of Information Sharing services made available through the Exchange.

The CJS Exchange provides 5 core types of Information Sharing services:

1. The 'Web and Google' of the CJS. The capability to access information currently locked away in the 1,000s of line of business systems of CJOs through technology we are all familiar with – the Web and search engines;

- for example the XHIBIT Web Portal which provides instant relays of Crown Court case progress to Crown Court staff, the public and approved members of the wide criminal justice community via the XHIBIT Web site

- for example creating new information 'services' based on existing line of business systems databases which can be search and accessed via Web applications – a scenario illustrating this is provided in Appendix A ('Intelligent Enterprise' Proof of Concept)

2. Information sharing between IT systems of CJOs, enabling new functionality to be supported within a CJO or to automate new flows of work across CJOs;

- for example enabling the CPS to receive initial case file information from the police – sharing case information between the police's NSPIS case preparation IT system and the CPS's COMPASS national case management IT system

3. Subscription and notification for people and IT systems;

- for example, through a police officer subscribing via a Web portal and 'RSS' (Really Simple Syndication), real-time news feed to the police officer's Web browser advising of the release from prison of offenders within their area, or an email notification of releases

- for example, through a citizen subscribing via a Web portal enabling a text message or email to be sent to a victim or witness advising the outcome of a particular crown court case

- for example, through configuring a subscription via a police IT system, automatically scheduling a police officer to visit a victim based on the outcome of a crown court case

4. Support for different types of IT systems and 'access devices' (e.g. desktop PCs and mobile devices) – i.e. 'multi-channel' support;

- for example enabling existing (often older technology) IT systems to interface with newer technology IT systems

- for example enabling the same information to be made available to an existing line of business system terminal or PC, to a Web browser or to a mobile PDA

5. Delivering the above services *in combination*; enabling potentially any information which is shared to be:

- searchable via Google or a like Search engine
- accessed via Web portals
- sent between IT systems
- subscribed to by a Public Servant or a Citizen
- subscribed to by any IT system

Functionality based on the information can be created once and used by IT systems across the CJS.

Information can be both a business event (e.g. offender released from prison) and business content (e.g. the name and address of the offender and their offending history). The same information shared via the Exchange originally for the purpose of viewing via a Web portal can for example be sent to multiple IT systems for their use through a subscription, enabling new functionality to be created in existing CJO line of business systems.

It is important to note that to avoid creating 'islands' of information sharing (which would present barriers to information sharing across the CJS) and to maximise the efficiency and effectiveness benefits of the Exchange as a shared service, use of the Exchange as opposed to CJO's creating their own similar services is key.

Appendix A – Scenario for Illustration Purposes - Police Investigation

This scenario illustrates the Information Sharing Operating Model, existing information sources of CJOs and the Exchange Shared Service in action. The scenario is presented at a high-level and is for illustration purposes only.

A robbery has taken place at a store, shots have been fired and Mark Bastin has been seriously injured. Three robbers were involved, two have escaped in a vehicle however Frank Barclay (who looks to be in his 60's) has been caught nearby but has no gun.

Police radios control centre to find possible leads to quickly start investigation.

Currently the officer would need to confirm the robber's details with the control room, and would not have easy access to information regarding risks, convictions and intelligence and other residents at that address.

Having adopted the Information Sharing Approach and implemented a new Web 'portal' to support Investigation activity, the police officer is now able to:

- *Call control centre who quickly search and retrieve all relevant data stores through a single Web portal (the officer could also do this using voice or PDA)*
- *Identify person and related warnings, known associates, convictions and locations*
- *Quickly build a full picture of the scene and send other officers to related locations*

Here is how the Information Sharing Approach and the Exchange would support this new outcome leveraging the existing information in CJO line of business systems:

1. The community of interest is Investigation. The Police Service wishes to establish this community and use the following existing Information Sources (currently locked away in various line of business systems):

   Electoral Register – name and address of all registered at that address
   SID (Scottish Intelligence Database) – previous convictions, risks, intelligence regarding all at address, warnings
   LIBRA (Magistrate's Court Case Management)– previous court appearances, outcomes and outstanding fines for all at address
   PNC (Police National Computer) – previous offences, details of all at address, warnings
   OASys (Offender Assessment System) – risks, convictions, warning signals
   ANPR (Automatic Number Plate Recognition)

2. The Police Service makes a request to each of the Information Owners above.

3. An Interchange Agreement is defined between the Information Owners which is signed-up to by all. The Information Owners agree that the Police Service can view their information for the purpose of investigation. Information Owners update their Data Protection Registrations appropriately. The Interchange Agreement is governed through representatives of each Information Owner chaired by the Police Service. The Interchange Agreement is established with the assistance of the CJSE Data Standards Forum, the Data Sharing Forum and the Information Security Forum.

4. In this case all the Information Owners have agreed that the Police Service can identify and authenticate their own officers to access the information for the purpose of investigation, and that the information can be accessed over a restricted end-end infrastructure.

5. The CJSE Data Standards Forum is engaged and an 'Investigation' Data Standards sub-group is created. This sub-group in combination with the forum agree that information sources will be used as is (i.e. based on their individual data standards) and the technology of the Exchange will be used to rapidly create a 'meta' model for information interchange to identify relationships between the disparate information sources – thereby enabling information to be searched and viewed across all the information sources in a rapid manner. The sub-group and forum define which interchange items within the 'meta' model are within standards, which are not and why, and define the roadmap for migration toward agreed standards to ensure cost-efficient sustainability and re-use potential of this specific solution. Appropriate use of interim data transformations are agreed to assist the standardisation process.

6. The Exchange Strategic Architecture (the Information Sharing Reference Enterprise Architecture) is used as input to define the Enterprise Architecture (business and IT blueprint) for the new Web portal application and the end-end integration architecture. Components of the Exchange are re-used with the specific configurations necessary to support this application.

7. So as not to adversely impact line of business systems of the Information Owners which the information sources currently support, either existing system interface mechanisms (such as Web Services) are used to access information sources (where these interfaces are able to support additional queries), or copies of the information sources are created which are hosted on the Exchange central platform. Update mechanisms are implemented to provide timely updates of the copies without impacting existing systems operations.

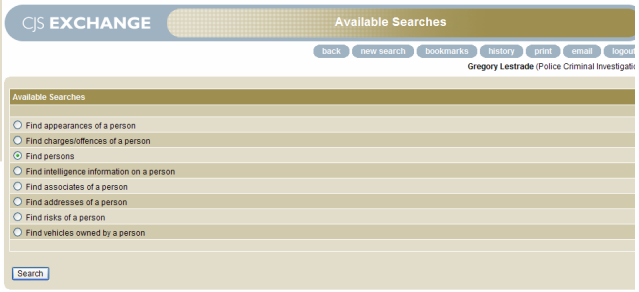
8. Using the services of the Exchange an Investigation Web Portal application is delivered in an affordable and timely fashion to provide functionality including searching and viewing of the combined information.

9. Note that, with appropriate approval from information owners through Interchange Agreements, the same information can be made available to other communities of interest via the Exchange, for example via other Web Portal applications or as Web Services components which CJOs can make use of to enhance their existing line of business systems.

Screen shots from the Investigation Web Portal application are shown below. This Web Portal application is in proof of concept on the Exchange[4] and is running off extracted, sanitised data from the Electoral Register, SID, LIBRA, PNC, OASys and ANPR.

[4] Up-to-date information on operational Information Sharing services enabled via the Exchange can be found at http://www.cjit.gov.uk/in-your-area/

Searching for 'Frank Barclay'



Selecting and viewing information about 'Frank Barclay'