A Overview of the National Criminal Justice Index

Prepared for:
Information Security and Privacy Advisory Board (ISPAB) Meeting
June 10-12, 2003
Rockville, MD

Presentation by: Tim Bouma
Senior Consultant,
CGI Management Consulting Group
Ottawa, Canada
mailto:tim.bouma@cgi.com
Tel: (613) 234-2155 Fax: (613) 234-6934
Presentation Outline

- NCJI Overview
- Data Integrity & Privacy
- Risk and Governance Analysis
- Privacy Impact Assessment
- Governance-Based Access Control
- NCJI MOU Details
- Conclusions
Presentation Outline

- NCJI Overview
- Data Integrity & Privacy
- Risk and Governance Analysis
- Privacy Impact Assessment
- Governance-Based Access Control
- NCJI MOU Details
- Conclusions
National Criminal Justice Index

- Solicitor General Integrated Justice Initiative (IJI)
  - Part of the Canadian Public Safety Information Network (CPSIN)
  - Primary goal to enhance public safety through better information sharing between agencies.

- Key Requirements
  - Establish a centralized index for information sharing between federal, provincial, and municipal agencies
  - Accommodate a wide variety of participants in the NCJI Program beyond the criminal justice community
  - Comply with Federal, Provincial Privacy and related legislation
## NCJI Stakeholder and Legislative Overview

<table>
<thead>
<tr>
<th>Stakeholder Major Interests (below)</th>
<th>NCJI Custodian</th>
<th>NCJI User</th>
<th>Citizen of Canada</th>
</tr>
</thead>
</table>
|                                     | *Agency that is responsible for the operation of NCJI* | *Any user that uses NCJI in support of their business processes (as mandated by their agency)* | **Primary Interests:**  
  • Public Safety/Security  
  • Protection of Rights and Freedoms |

### Rights (or Powers)

<table>
<thead>
<tr>
<th></th>
<th>NCJI Custodian</th>
<th>NCJI User</th>
<th>Citizen of Canada</th>
</tr>
</thead>
</table>
|                                        |                | *Agency-Specific Legislation*  
  e.g.  
  • RCMP Act  
  • Customs Act  
  • Immigration and Refugee Protection Act | *Charter of Rights and Freedom*  
  • Young Offenders Act  
  • Access to Information Act  
  • Privacy Act  
  • Personal Information Protection and Electronic Documents Act |                     |

<table>
<thead>
<tr>
<th>Responsibilities (or Obligations)</th>
<th>NCJI Custodian</th>
<th>NCJI User</th>
<th>Citizen of Canada</th>
</tr>
</thead>
</table>
|                                       | *Access to Information Act*  
  • Privacy Act  
  • Personal Information Protection and Electronic Documents Act  
  • Charter of Rights and Freedoms  
  • Criminal Records Act  
  • Identification of Criminals Act  
  • Young Offenders Act  
  • Witness Protection Program Act  
  • National Archives Act | *same as column to the left* |                     |
The More General Challenge...

- In the efforts to increase public safety and security, government agencies are being urged to:
  1. Be more effective and efficient through more coordinated (or less fragmented) approaches to law enforcement, protection, security, etc.
  2. Key to the above is the sharing of information across systems, agencies, and jurisdictions

- But many risk associated with information sharing due to:
  - Legislative compliance
  - Lack of clear accountability structures, unknown liabilities,
  - Privacy rights of individuals
  - Data Integrity (personal information)
  - Unauthorized/Unintended Data Matching/Data Linkage

- Current agency systems and processes are not well set-up
  - To pro-actively share information beyond their security regimes.
  - To manage or contain the above risks
Presentation Outline

- NCJI Overview
- Data Integrity & Privacy
- Risk and Governance Analysis
- Governance-Based Access Control
- NCJI MOU Details
- Conclusions
Data Integrity - NCJI

- Publishing agencies responsible for data integrity.
  - Throughout entire lifecycle – including disposition of information assets
- Investigators cannot assume:
  - The data is correct
  - Or, even if it’s the right data!
- Must confirm with publishing agency before they can act on information
  - Agency Contact Information presented along with each hit
  - Index Scoring used to present a standard level of confidence
Data Integrity - CPIC

- Not a substitute for police officer’s judgment
- A hit is only an indication of probability or “lead” information until confirmed.
- In every case, enquiring agencies must verify accuracy of record with originating agency (HIT CONFIRMATION)
- Originating agency is responsible for validity, relevance, and quality of data input
- CPIC Records must be validated by originating agencies on a recurring basis
NCJI Privacy Impact Assessment

- All new federal programs are required to conducted Privacy Impact Assessment (PIA)
  - Approximately 50 Federal PIA’s have been conducted
- NCJI has conducted Preliminary PIA (PPIA)
- NCJI PPIA Key Recommendations:
  - Consent:
    - no victim/witness information to be shared
  - Use of Personal Information
    - Ensure Agencies do not have access information beyond their mandate (enforced via RBAC – Roles /GBAC – Governance Attributes)
  - Accuracy of Personal Information
    - NCJI information is not actionable, must be confirmed with provider agency
    - NCJI must be accurate, as up-to-date as possible
  - No Data Matching/ Linkage
    - NCJI only returns a series of ‘locators’ to originating systems
Presentation Outline

- NCJI Overview
- Data Integrity & Privacy
- Risk and Governance Analysis
- Governance-Based Access Control
- NCJI MOU Details
- Conclusions
# Information Sharing Risks

<table>
<thead>
<tr>
<th>Collection (within Agency)</th>
<th>Maintenance and Protection</th>
<th>Dissemination &amp; Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publishing Agency is accountable</td>
<td>Publishing Agency is accountable</td>
<td>Publishing Agency is accountable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Subscribing Agency is accountable Publishing Agency is also accountable</td>
</tr>
</tbody>
</table>

**Agencies assume the majority of risk when they publish or disclose information. Risk and perception of risk are the single largest barriers to information sharing.**

**Note:** Risk in this context is primarily the possibility of direct or indirect non-compliance of an agency due to: 1) improper disclosure, 2) improper use, and, 3) data integrity.
Governance Analysis

Legislation/Jurisdiction

- Regulations
- Rulings
- Precedents
- Programs, Policies
- Agreements
- Standard Operating Procedures

Agency Mandate

used to institute

Business Processes

supported by the following (information-intensive) activities

Creation & Collection
Maintenance & Protection
Dissemination & Use
Preservation, Retention & Disposal

and is held as various

Information Assets
Governance Analysis

Legislation/Jurisdiction

Agencies, Information Systems

Information Asset <Attributes>

Simplifying Assumption...

... because ultimate accountability must map back to the relevant legislation and jurisdiction

This level of detail/complexity can be removed from final specifications...
Preliminary Conclusions

1. The use of information assets, regardless of agency or system, shared or not shared, must always be subject to its *originating governance* (ultimately, legislation).

2. To ensure compliance, information assets must be explicitly categorized according to their relevant legislation and jurisdictions (not by agency, system, etc.)

3. Rules for access/use should also be based on legislation/jurisdiction.
Presentation Outline

- NCJI Overview
- Data Integrity & Privacy
- Risk and Governance Analysis
- Governance-Based Access Control
- NCJI MOU Details
- Conclusions
Governance Based Access Control

- Governance-Based Access Control (GBAC) is an approach to:
- Enhance information sharing by providing a common framework to ensure governance as information assets are being shared across agencies and jurisdictions by means of:
  1. A common way to *classify information assets* according to its intended purpose, namely through its governing legislation
  2. A common way to associate *rules of governance and enforce access* to information assets, regardless of where they reside (system, agency, etc.)
# GBAC Classification Scheme

*Governance Attributes used for information classification*

<table>
<thead>
<tr>
<th>Governance Attribute</th>
<th>Description/Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Jurisdiction</td>
<td>Distinguishing name of the jurisdiction (e.g. &quot;Ontario&quot;, &quot;Canada&quot;, &quot;Michigan&quot;, etc) that has collected information for the purposes of creating a primary information asset. <em>(primary, meaning it is ultimately responsible)</em></td>
</tr>
<tr>
<td>2. Collection Authority</td>
<td>Statute of authority under which information is <strong>collected and used</strong> <em>(including subsequent use)</em> for law enforcement, investigative, and/or administrative enforcement purposes.</td>
</tr>
<tr>
<td>3. Collection Reason</td>
<td>The direct operating program or activity under which the information asset was created (e.g Dispatch, Investigation, Court Liaison, etc.).</td>
</tr>
<tr>
<td>4. Security Designation</td>
<td>As per government information security and information sensitivity policies</td>
</tr>
<tr>
<td>5. Disclosure Authority</td>
<td>Statute of authority under which information maybe <strong>disclosed</strong> for subsequent use. Assumption is that this statute is in same jurisdiction as the Collection Authority</td>
</tr>
<tr>
<td>6. Disposition Authority</td>
<td>Statute of authority under which information must be retained and eventually disposed. <em>(For Federal agencies, this would normally be the National Archives Act. )</em></td>
</tr>
</tbody>
</table>
# Example of GBAC Classification

<table>
<thead>
<tr>
<th>Governance Attribute</th>
<th>Example Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Jurisdiction</td>
<td>CA&lt;br&gt;NF,NS,PEI, NB,PQ&lt;br&gt;ON,MB&lt;br&gt;SK,AB,BC&lt;br&gt;YK,NWT,NV</td>
</tr>
<tr>
<td>2. Collection Authority</td>
<td>CA-Criminal-Code&lt;br&gt;CA-Customs-Act&lt;br&gt;CA-Immigration-Refugee-Protection-Act</td>
</tr>
<tr>
<td>3. Collection Reason</td>
<td>Police Investigation&lt;br&gt;Border Inspection&lt;br&gt;Examination of Goods</td>
</tr>
<tr>
<td>4. Security Designation</td>
<td>Protected A&lt;br&gt;Protected B</td>
</tr>
<tr>
<td>5. Disclosure Authority</td>
<td>Privacy Act&lt;br&gt;Customs Act&lt;br&gt;Young Offenders Act</td>
</tr>
<tr>
<td>6. Disposition Authority</td>
<td>National Archives Act</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GBAC CLASSIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jurisdiction</td>
</tr>
<tr>
<td>Collection Authority</td>
</tr>
<tr>
<td>Collection Reason</td>
</tr>
<tr>
<td>Security Designation</td>
</tr>
<tr>
<td>Disclosure Authority</td>
</tr>
<tr>
<td>Disposition Authority</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GBAC CLASSIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jurisdiction</td>
</tr>
<tr>
<td>Collection Authority</td>
</tr>
<tr>
<td>Collection Reason</td>
</tr>
<tr>
<td>Security Designation</td>
</tr>
<tr>
<td>Disclosure Authority</td>
</tr>
<tr>
<td>Disposition Authority</td>
</tr>
</tbody>
</table>
Presentation Outline

- NCJI Overview
- Data Integrity & Privacy
- Risk and Governance Analysis
- Governance-Based Access Control
- NCJI MOU Details
- Conclusions
# Information Sharing Risks

<table>
<thead>
<tr>
<th>Collection (within Agency)</th>
<th>Maintenance and Protection</th>
<th>Dissemination &amp; Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publishing Agency is accountable</td>
<td>Publishing Agency is accountable</td>
<td>Publishing Agency is accountable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Subscribing Agency is accountable Publishing Agency is also accountable</td>
</tr>
</tbody>
</table>

![Publishing Agency Risk](image)
# MOU Balances the Risk

<table>
<thead>
<tr>
<th>Collection (within Agency)</th>
<th>Collection (within Agency)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publishing Agency is accountable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Maintenance and Protection</th>
<th>Primary Use (within Agency)</th>
<th>Publishing Agency is accountable</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dissemination &amp; Use</th>
<th>Disclosure (to other Agencies)</th>
<th>Publishing Agency is accountable</th>
<th>Subsequent Use (by other Agencies)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Publishing Agency is accountable</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Publishing Agency Risk**

**Define Scope of Information**

**Classify Information**

**Use of Information Assets**

**Subscribing Agency Risk**

---

[Image: MOU Balances the Risk diagram]
NCJI Draft MOU re: Data Accuracy

- Information remains property of, and remains in control by NCJI Provider Agency.
- Accuracy of Information Provided to NCJI
  - NCJI Provider Agency takes all reasonable steps to ensure information is accurate
  - If information is discovered to be inaccurate, NCJI Agency to advise agency who controls information
  - If no resolution between parties, NCJI Administrator will make every effort to effect resolution
- Accuracy of Information Accessed via NCJU
  - same as conditions as above
# MOU Sections

MOU Sections required to be completed to ensure proper accountability between participating publishing and subscribing agencies. These would become part of the MOU.

<table>
<thead>
<tr>
<th>MOU Section</th>
<th>Purpose of Section</th>
<th>Accountability</th>
</tr>
</thead>
</table>
| Scope of Information Assets to be shared | **To identify and agree upon:**  
1) The valid and appropriate governance attributes applicable to an agency's information assets | • To ensure the publishing agency has the power to collect and disclose information that may be used by subscribing agencies. |
| Classification of Information Assets to be shared | **To identify and agree upon:**  
1) Which agency information assets will be shared/published via NCJI  
2) How these information assets will be classified according to the agreed upon governance attributes | • To ensure the publishing agency has properly considered which information assets may (or may not) be disclosed to subscribing agencies.  
• To ensure published information assets are properly classified such that they can only be used in a consistent manner by subscribing agencies |
| Use of Shared Information Assets         | **To identify and agree upon:**  
1) Which agency job functions qualify and map to which NCJI roles | • To ensure subscribing agencies are allowing access to designated individuals.  
• To ensure that these individuals, according to their job functions are using the information assets in a legal and consistent manner |
MOU: Scope of Information

Purpose of Worksheet:
Ensures agencies are accountable for the type of information they collect and will disclose via NCJI
Key elements that must be identified and agreed upon:
1. Nature and scope of agency information to be shared. This is achieved by the identification of the valid and appropriate governance attributes applicable to an agency’s information assets.

Example Requirements Worksheet:

<table>
<thead>
<tr>
<th>Agency Worksheet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agency:</td>
</tr>
<tr>
<td>&lt;Name of Participating Agency&gt;</td>
</tr>
<tr>
<td>Valid Governance Attributes</td>
</tr>
<tr>
<td>Jurisdiction</td>
</tr>
<tr>
<td>&lt;List of Valid Attributes&gt;</td>
</tr>
</tbody>
</table>

Approved by:
Agency Head: __________________
NCJI Governance: ______________
MOU: Classification of Information Assets

Purpose of Worksheet:
Ensures agencies properly classify information so that upon disclosure it is used consistently with its initial purpose.

Key elements that must be identified and agreed upon:
1) Which specific agency information assets that will be shared/published via NCJI
2) How these information assets will be classified according to the agreed upon governance attributes

<table>
<thead>
<tr>
<th>Agency Information Asset Worksheet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publishing Agency:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Agency Information Asset</th>
<th>NCJI Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ref. No.</td>
<td>Information Asset Description</td>
</tr>
<tr>
<td>1.</td>
<td>&lt;Description of asset type to be Published to NCJI&gt;</td>
</tr>
<tr>
<td>2.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td></td>
</tr>
</tbody>
</table>

Approved by:
Agency Head: ______________________
NCJI Governance: ______________________
# MOU: Use of Information Assets

**Purpose of Worksheet:**
Ensures agencies properly use information that has been disclosed by publishing agency

Key elements that must be identified and agreed upon:
1) Local Authority
2) Which agency job functions qualify for which NCJI roles

<table>
<thead>
<tr>
<th>Agency Job-Title Worksheet</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Agency:</strong></td>
</tr>
<tr>
<td>&lt;Name of Participating Agency&gt;</td>
</tr>
<tr>
<td><strong>Local Authority:</strong></td>
</tr>
<tr>
<td>&lt;Name and/or Job-Function of Agency Personnel&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Agency Job Functions</th>
<th>NCJI Role Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ref. No.</td>
<td>Agency Job Function and Description</td>
</tr>
<tr>
<td>1.</td>
<td>&lt;Agency Job Title and Description&gt;</td>
</tr>
<tr>
<td>2.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td></td>
</tr>
</tbody>
</table>

Approved by:
Agency Head: ______________
NCJI Governance: ______________
Presentation Outline

- NCJI Overview
- Data Integrity & Privacy
- Risk and Governance Analysis
- Governance-Based Access Control
- NCJI MOU Details
- Conclusions
Conclusions

- Better information sharing has now become a priority for all government agencies
- NCJI is a first step to better information sharing between agencies in the criminal justice community
  - Many issues/risks related to compliance, privacy, data integrity
- Common information sharing standards and frameworks are only now emerging
  - RBAC, GBAC, XACML
Questions?