

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

	Primary Stakeholder Types		
	NCJI Custodian	NCJI User	Citizen of Canada
Stakeholder Major Interests (below)	<i>Agency that is responsible for the operation of NCJI</i>	<i>Any user that uses NCJI in support of their business processes (as mandated by their agency)</i>	Primary Interests: <ul style="list-style-type: none"> •Public Safety/Security •Protection of Rights and Freedoms
Rights (or Powers)		<ul style="list-style-type: none"> •Agency-Specific Legislation e.g. •RCMP Act •Customs Act •Immigration and Refugee Protection Act 	<ul style="list-style-type: none"> •Charter of Rights and Freedom •Young Offenders Act •Access to Information Act • Privacy Act • Personal Information Protection and Electronic Documents Act
Responsibilities (or Obligations)	<ul style="list-style-type: none"> •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 be 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

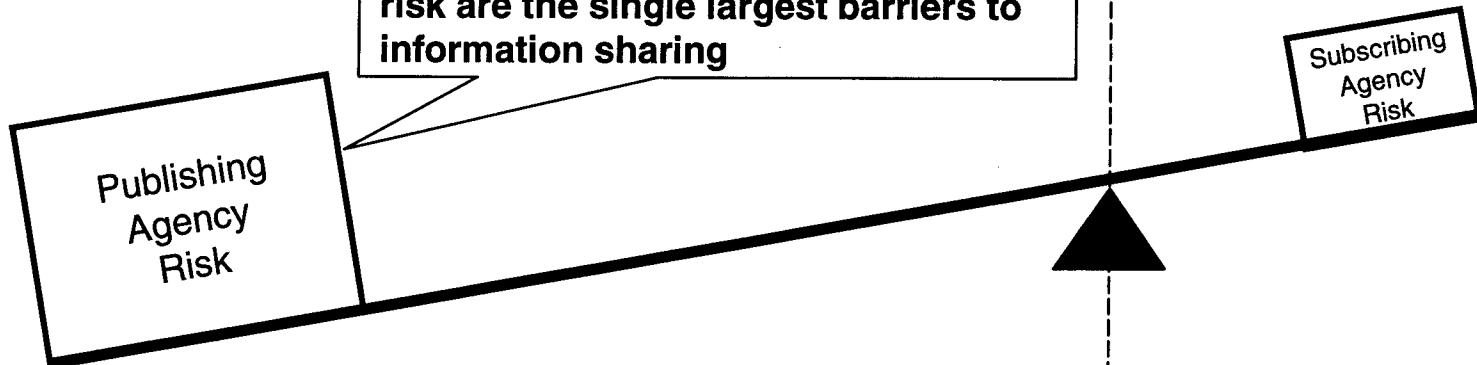
Presentation Outline

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

Information Sharing Risks

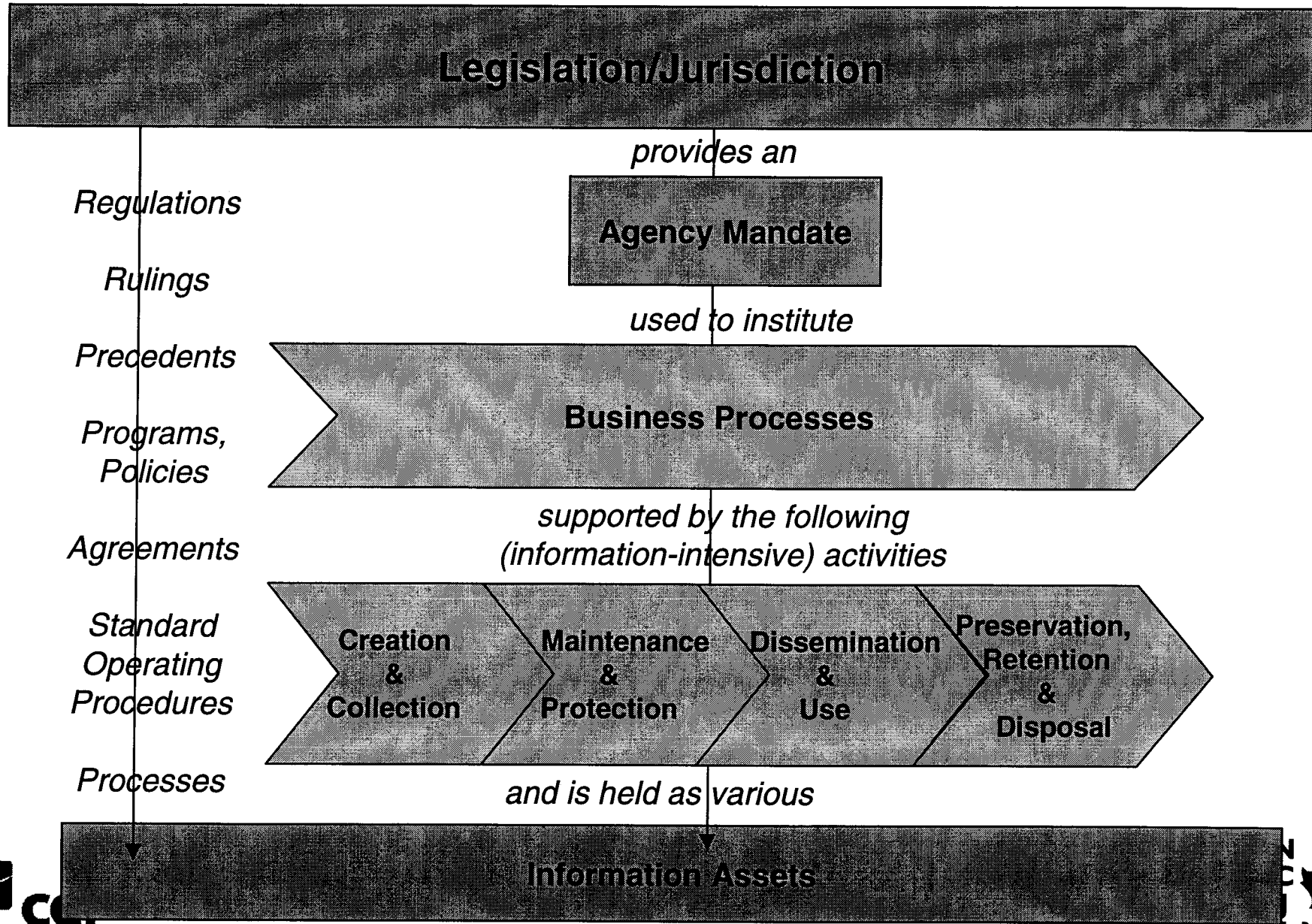
Collection	Maintenance and Protection	Dissemination & Use	
Collection (within Agency)	Primary Use (within Agency)	Disclosure (to other Agencies)	Subsequent Use (by other Agencies)
Publishing Agency is accountable	Publishing Agency is accountable	Publishing Agency is accountable	Subscribing Agency is accountable Publishing Agency is also accountable

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

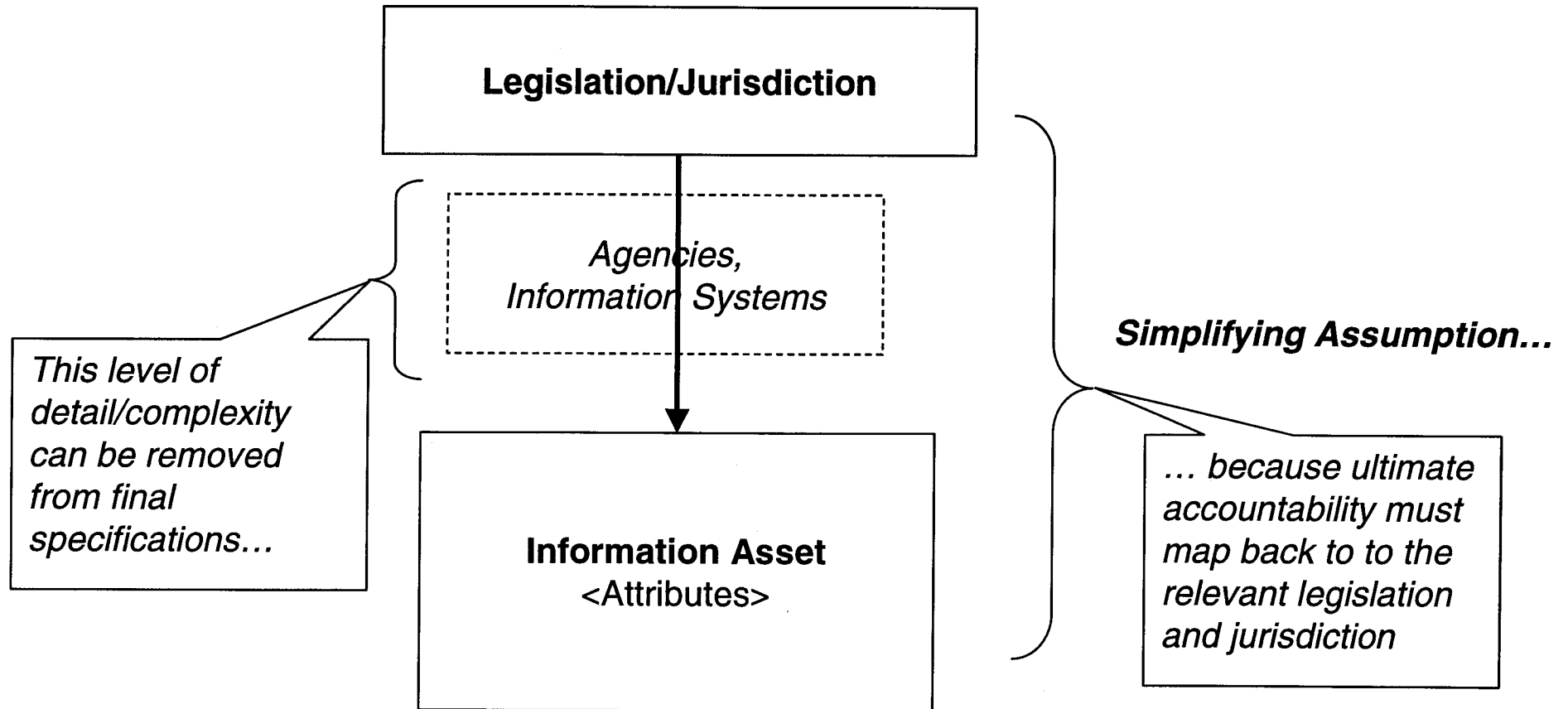


Note: Risk in this context is primarily the possibility of direct or indirect non-compliance of an agency due to: 1) improper disclosure, 2) improper use, and, 3) data integrity

Governance Analysis



Governance Analysis



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

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

Example of GBAC Classification

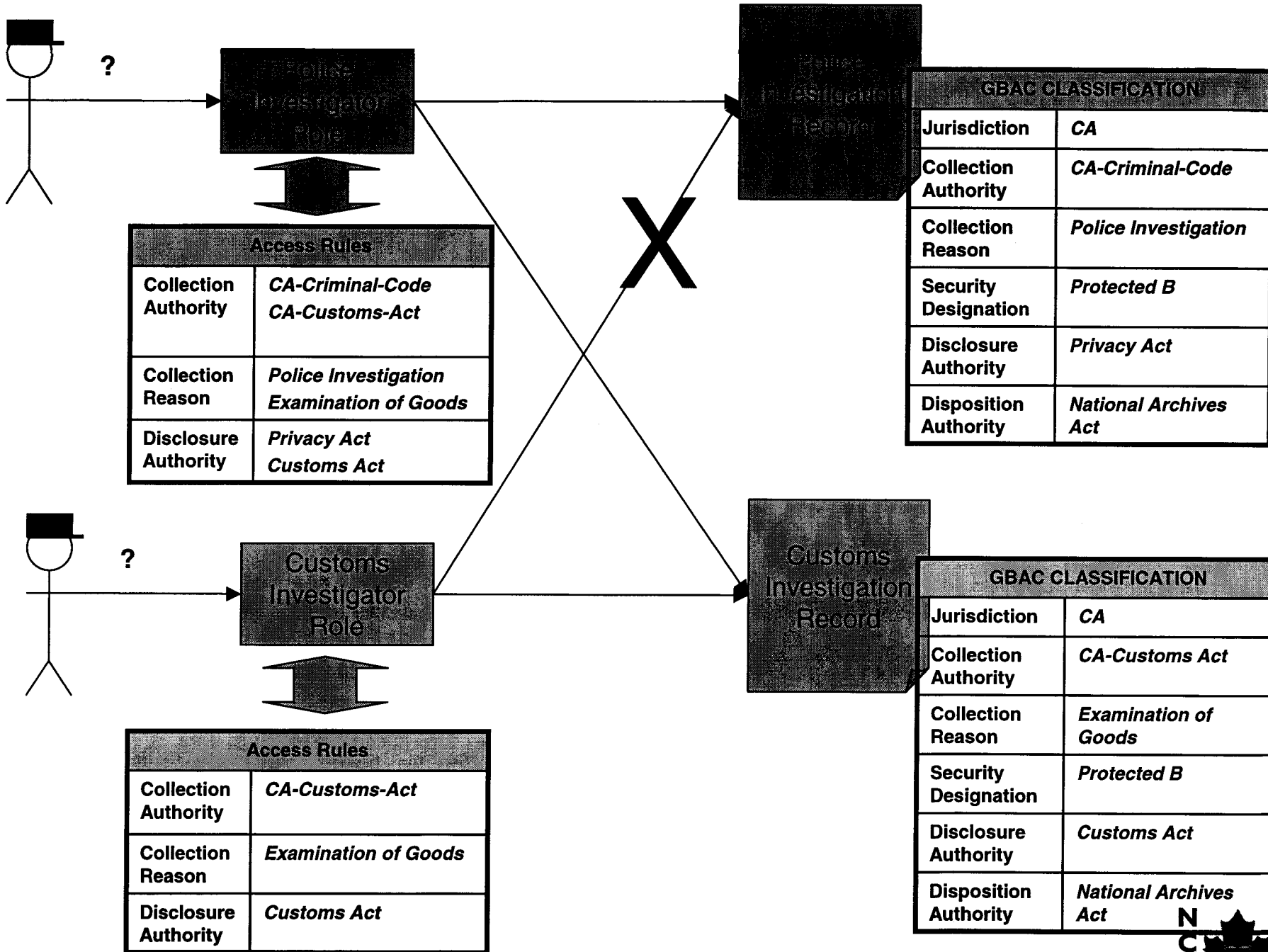
Governance Attribute	Example Values
1. Jurisdiction	CA NF,NS,PEI, NB,PQ ON,MB SK,AB,BC YK,NWT,NV
2. Collection Authority	CA-Criminal-Code CA-Customs-Act CA-Immigration-Refugee-Protection-Act
3. Collection Reason	Police Investigation Border Inspection Examination of Goods
4. Security Designation	Protected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

Police
Investigation
Record

GBAC CLASSIFICATION	
Jurisdiction	CA
Collection Authority	CA-Criminal-Code
Collection Reason	Police Investigation
Security Designation	Protected B
Disclosure Authority	Privacy Act
Disposition Authority	National Archives Act

Customs
Investigation
Record

GBAC CLASSIFICATION	
Jurisdiction	CA
Collection Authority	CA-Customs Act
Collection Reason	Examination of Goods
Security Designation	Protected B
Disclosure Authority	Customs Act
Disposition Authority	National Archives Act

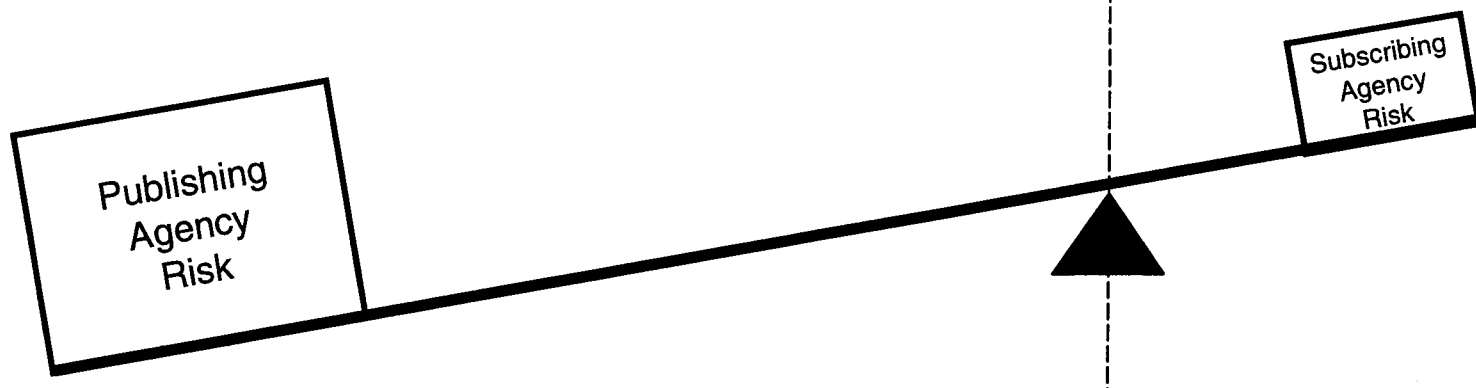


Presentation Outline

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

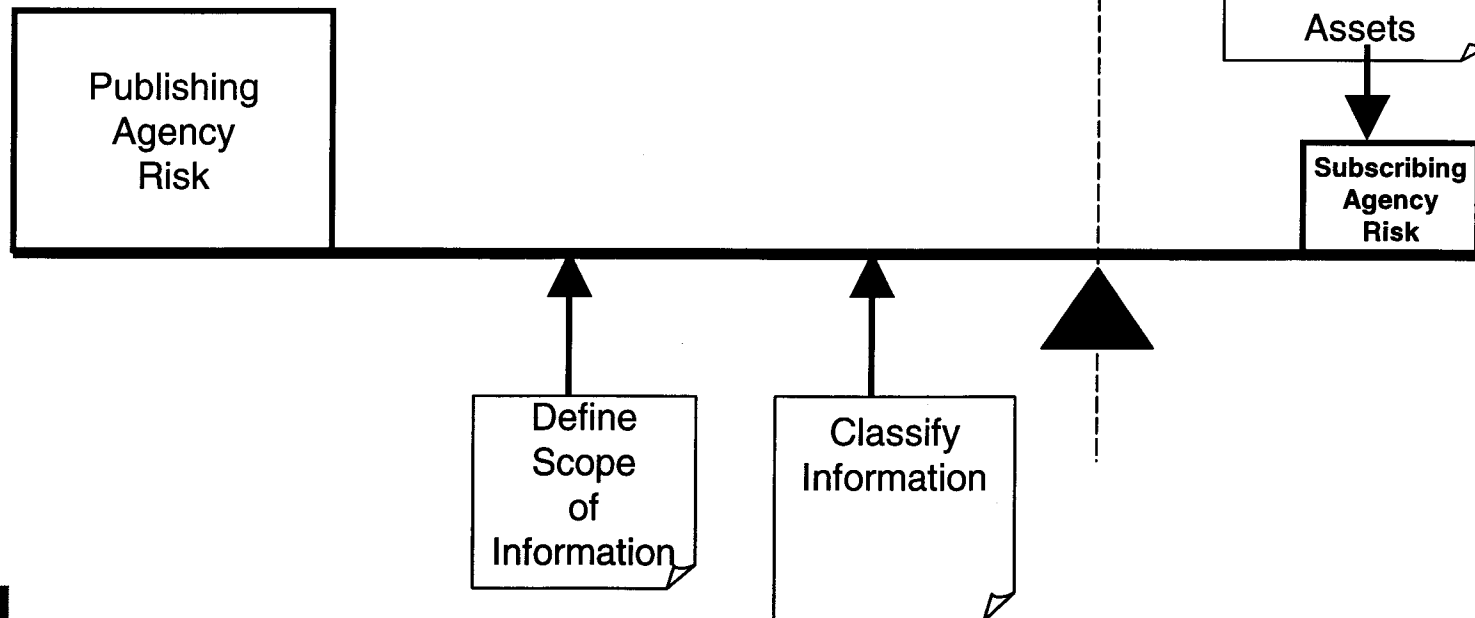
Information Sharing Risks

Collection	Maintenance and Protection	Dissemination & Use	
Collection (within Agency)	Primary Use (within Agency)	Disclosure (to other Agencies)	Subsequent Use (by other Agencies)
Publishing Agency is accountable	Publishing Agency is accountable	Publishing Agency is accountable	Subscribing Agency is accountable Publishing Agency is also accountable



MOU Balances the Risk

Collection	Maintenance and Protection	Dissemination & Use	
Collection (within Agency)	Primary Use (within Agency)	Disclosure (to other Agencies)	Subsequent Use (by other Agencies)
Publishing Agency is accountable	Publishing Agency is accountable	Publishing Agency is accountable	Subscribing Agency is accountable Publishing Agency is also accountable



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

MOU Section	Purpose of Section	Accountability
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	<ul style="list-style-type: none"> •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	<ul style="list-style-type: none"> •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	<ul style="list-style-type: none"> •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:

Agency Worksheet						
Agency:		<Name of Participating Agency>				
Valid Governance Attributes						
Jurisdiction	Collection Authority	Collection Reason	Disclosure Authority	Security Designation	Disposition Authority	
<List of Valid Attributes>	<List of Valid Attributes>	<List of Valid Attributes>	<List of Valid Attributes>	<List of Valid Attributes>	<List of Valid Attributes>	
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

Agency Information Asset Worksheet						
Publishing Agency:		<Name of Participating Agency>				
Agency Information Asset				NCJI Classification		
Ref. No.	Information Asset Description	Security Designation	Publish to NCJI?	Governance Attributes		Agreed-Upon Values for Information Asset
1.	<Description of asset type to be Published to NCJI>	<Agency Level Designation >	<Y/N>	1.	Jurisdiction	1. _____
				2.	Level of Jurisdiction	2. _____
				3.	Collection Authority	3. _____
				4.	Collection Reason	4. _____
				5.	Security Designation	5. _____
				6.	Disclosure Authority	6. _____
				7.	Disposition Authority	7. _____
2.				1.	Jurisdiction	1. _____
				2.	Level of Jurisdiction	2. _____
				3.	Collection Authority	3. _____
				4.	Collection Reason	4. _____
				5.	Security Designation	5. _____
				6.	Disclosure Authority	6. _____
				7.	Disposition Authority	7. _____

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

Agency Job-Title Worksheet				
Agency:		<Name of Participating Agency>		
Local Authority:		<Name and/or Job-Function of Agency Personnel>		
Agency Job Functions			NCJI Role Assignment	
Ref. No	Agency Job Function and Description	Description of Reason(s) and Relevant Authorities	NCJI Role Assignment ?	Authorized NCJI Role(s)
1.	<Agency Job Title and Description>	<Reasons why and Relevant Authorities>	<Y/N>	<List of NCJI Roles>
2.				
3.				

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?

