

# FOCUS ON PRIVACY OSS PRIVACY

***The Ontario Shared Services Privacy Review***

***Presented by Estella Cohen and David Jackson***

***ACCESS & PRIVACY WORKSHOP 2006***

***Sept 14 & 15, 2006***

***Queen's Park, Toronto, Ontario***

# Agenda & Objectives for Today's Session

## AGENDA:

- Privacy Breach @ OSS ....journey from Crisis to Confidence

## SESSION OBJECTIVES:

- Privacy Review Process
- Development of Privacy Standard
- Benchmarking key operational areas
- Recommendations
- Implementation/ Progress to date
- Our Contact Info

# The OSS Privacy Review

- Probably the largest public sector privacy review at this level of detail that has ever been conducted in Canada.
- Resulted in the first public sector based privacy standard in Canada.
- For Ontario Shared Services (OSS) it has taken the guesswork out of privacy compliance, and has moved the organization from crisis to confidence in the area of protection of personal information.

# What is Ontario Shared Services

- OSS delivers enterprise-wide internal business support and supply chain management services on behalf of the Ontario government to ministries and agencies across the Ontario Public Service, as well as a host of other common enterprise wide services such as mail, print, insurance and risk management, translation services, retention and storage of of government records.
- ✓ \$4 billion annual payroll affecting over 70,000 public servants
  - ✓ Accounts receivable of \$ 1 Billion
  - ✓ Purchase transactions of \$144 million
  - ✓ Travel transactions of \$117 Million
  - ✓ Management of 600 vendor contracts affecting about \$1 Billion of annual procurements
  - ✓ Contact Centre handles in excess of 130,000 calls annually, include authentication and password resets
  - ✓ Manages the MyOPS portal with 2 million hits per annum
  - ✓ Manages 1.1 million cubic feet of records, 110,000 retrievals annually
  - ✓ Delivers 30,000 pieces of mail daily

# Scope

- Ontario Shared Services is the internal transactional services provider to the Ontario Public Service (OPS). The review was comprehensive of all of its business services:
  - ❖ Accounts Payable Processing
  - ❖ Advance Accounts Payment Processing
  - ❖ Collections Processing
  - ❖ Payroll and Benefits Administration
  - ❖ Procurement Services
  - ❖ General Administrative Services (forms management, translation, information storage and retrieval, mail and print, official documents, risk management and insurance)
- Major technology applications related to these functions include the Integrated Financial Information System (IFIS), based on Oracle Financials; Workforce Information System (WIN), based on PeopleSoft HR; and CORPAY, the corporate payroll system, based on Integral Systems Payroll.

# The Challenge

- To define and advance a standard for the protection of personal information, with reinforcing policies and practices, and to foster a privacy culture that supports Ontario Government business while meeting or exceeding the evolving privacy expectations of its citizens.

# Privacy Review

## Why OSS?

- Privacy breach involving 27,000 Ontarians during the processing of Ontario Child Care Supplement cheques resulted in the Information and Privacy Commissioner's report to the Legislature on December 16, 2004.
- In that report, the Information and Privacy Commissioner (IPC) called for an independent end-to-end audit of OSS functions, operations and privacy practices involving the handling of personal information.
- Report to be made public at completion and to be delivered to the IPC within eight months (August 16, 2005).

# Work Done Concurrently

➤ **Triage Analysis:**

Incidents and their remediation reviewed.

➤ **Information Gathering:**

OSS practices, procedures, operations and activities for handling personal information assessed.

➤ **Privacy Impact Assessments:**

All Privacy Impact Assessments within OSS were assessed, and outstanding Privacy Impact Assessments were identified and completed on a priority basis.

➤ **Standard Selection:**

An OSS Privacy Standard was developed (against which the OSS' privacy practices would be reviewed).

The Standard was developed through the work of OSS management and executives, the Privacy Review Working Group and Steering Committee, with special support from MBS Privacy Policy (Office of the Corporate Chief Information Officer) and MGS Legal Privacy group.



# OSS Privacy Standard: “FIPPA Plus”

- “FIPPA Plus” was selected and endorsed as the standard for the OSS Privacy Review.
- FIPPA Plus includes *not only* the legislative requirement of FIPPA (Freedom of Information and Protection of Privacy Act), *but also* (PLUS):
  - other legislation applicable to privacy elements (Public Service Act and Archives Act);
  - Policies informed by the IPC guidelines and direction; and
  - OPS Freedom of Information Directive (2/91), policies and procedures inherent in operationalizing the privacy requirements (e.g. training, material availability).
- Why FIPPA Plus?
  - FIPPA is the legal obligation for the OPS.
  - FIPPA Plus anticipates emerging best practices found in the Canadian Standards Association Model Code or the Generally Accepted Privacy Principles of the Canadian Institute of Chartered Accountants.



## Aligning with Fair Information Practices

- To transform FIPPA Plus into the language of an effective privacy standard, OSS developed measurable Management Assertions, Criteria, and Activities aligned with globally recognized Fair Information Practices.
- Fair Information Practices:
  - A set of policies, practices and procedures designed to ensure the fair, lawful and ethical collection, use and disclosure of personal information, which give respect to the rights of the individual.

# Privacy Standards

OSS Standard: FIPPA Plus	CSA Model Code	GAPP-CICA Standard
Management	Accountability	Management
Notice	Identifying Purpose	Notice
--	Choice and Consent	Choice and Consent
Collection	Limiting Collection	Collection
Limiting use	Limiting Use, Disclosure and Retention	Use and Retention
Limiting Disclosure		Disclosure
Disposition		Use and Retention
Accuracy	Accuracy	Quality
Safeguarding and Security	Safeguards	Security
Transparency	--	--
--	Challenging Compliance	--
Access and Correction	Individual Access, Access and Correction	Access, Monitoring and Enforcement

# OSS Privacy Standard: Management Assertions, Criteria and Activities

<b>Management Assertions:</b>	<i>Example: Management</i>
<ul style="list-style-type: none"> <li>➤ high-level statements, grounded in the Freedom of Information and Protection of Privacy Act</li> <li>➤ closely modeled on fair information principles</li> </ul>	<p><i>“OSS meets its obligations in an environment of shared responsibility for privacy.”</i></p>
<b>Criteria:</b>	<i>Example: Criterion 1</i>
<ul style="list-style-type: none"> <li>➤ statements designed to operationalize the assertions with respect to identifying <b>what</b> is specifically required to be undertaken by Ontario Shared Services.</li> </ul>	<p><i>“OSS takes responsibility for its own compliance with the requirements of law and corporate policy.”</i></p>
<b>Activities:</b>	<i>Example: Activity vii</i>
<ul style="list-style-type: none"> <li>➤ describe procedures and practices necessary to operationalize the criteria, and</li> <li>➤ <b>how</b> this may be accomplished.</li> </ul>	<p><i>“Employees receive privacy training.”</i></p>

# OSS Privacy Standard

**The OSS Privacy Standard's measurable activities (172 in total) can also be categorized by group:**

**Policy (30 activities)**

Measurable activities which demonstrate that the organization has defined and documented its policies relevant to the privacy criterion.

**Procedure (92 activities)**

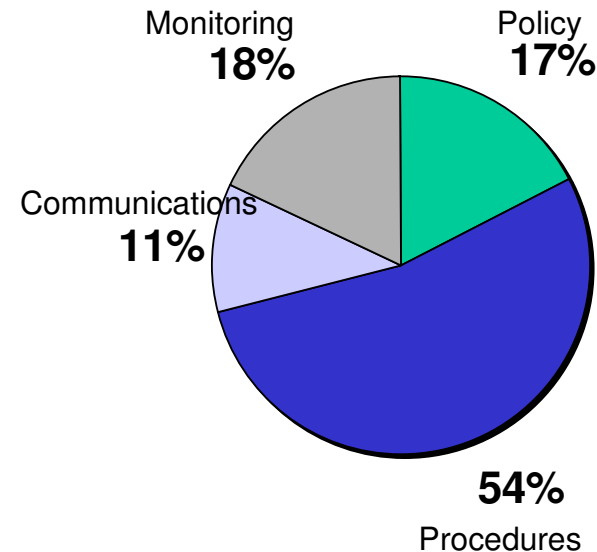
Measurable activities which demonstrate that the organization uses procedures to achieve its objectives in accordance with its defined privacy policies.

**Communications (19 activities)**

Measurable activities which demonstrate that the organization has communicated its defined policies to authorized users.

**Monitoring (31 activities)**

Measurable activities which demonstrate that the organization monitors the system and takes action to maintain compliance with its defined policies.



\*

# OSS Privacy Standard Development and Endorsement

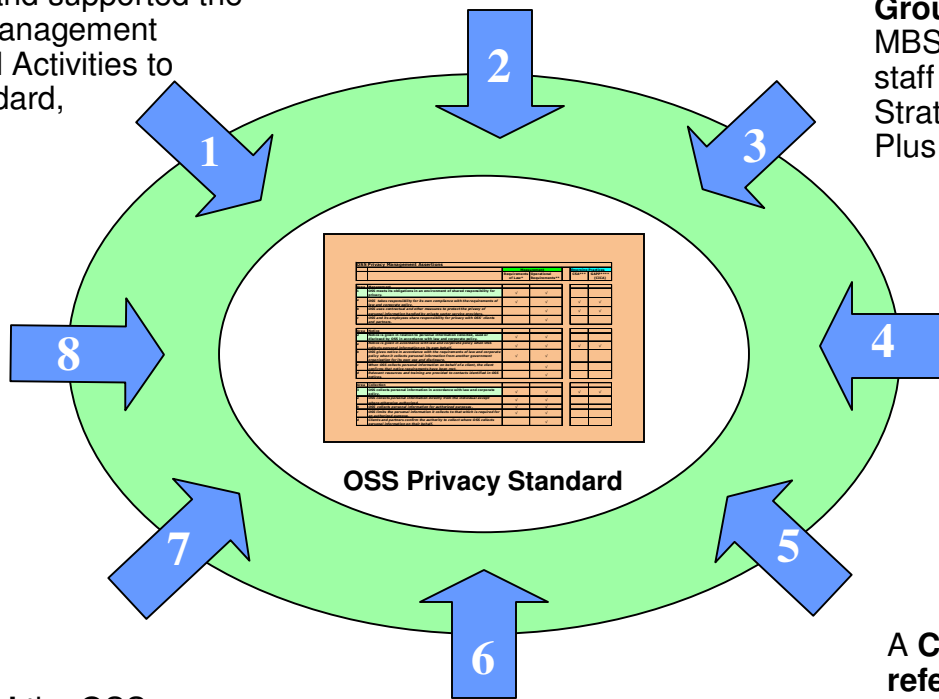


**Privacy Review Steering Committee approved in principle** the use of the FIPPA Plus standard, and supported the development of draft Management Assertions, Criteria and Activities to operationalize the standard,

An intensive effort began, to **operationalize FIPPA Plus** in terms that could be measured.

The **Privacy Review Project Working Group and Steering Committee**, MBS legal counsel and privacy policy staff (Office of the Chief Corporate Strategist) **reviewed** the draft FIPPA Plus standard.

**The Information and Privacy Commissioner** was briefed on the standard and endorsed the work of the project.



**OSS senior management** reviewed and **endorsed** the standard.



**Minister endorsed** the OSS Privacy Standard for the OSS Privacy Review .

The OSS Privacy Standard was **approved by the Steering Committee** and **endorsed by the Executive Sponsors**.

A **Chief Administrative Officers' reference group** and the **Chief Administrative Officers' Forum Executive** were **consulted** to understand the potential use of this methodology for the broader OPS.

# OSS Privacy Review Findings

- OSS meets the OSS Privacy Standard it is striving to achieve in some areas, but requires more attention in order to meet the Standard in the others.
- Privacy policies, procedures and guidance need to be strengthened to support the privacy obligations of OSS and their clients through:
  - More strongly articulated communications;
  - More effective ongoing monitoring at the procedural level; and
  - Improvement to privacy training - in amount, depth and scope – to ensure that a “privacy culture” is established and maintained.

## Findings: Privacy in a Horizontal World

- The model of shared accountability for privacy is a complex one, and requires focused leadership and improved understanding of where OSS business processes intersect with ministry processes in the management of personal information.
- It is important that someone be charged with the overall accountability for privacy within OSS.
- It is also important that OSS and its clients or third parties, such as contractors, clarify privacy responsibilities through Service Level Agreements.

## Findings: Privacy in a Horizontal World

- As an integral component of a large, complex organization, OSS must ensure that its privacy initiatives are coordinated and accepted by client ministries, and supported by corporate policy in order to effectively meet its privacy obligations and create a sustainable privacy culture.

# Report Conclusions

- Full compliance with the OSS Privacy Standard is a multi-year endeavour, supported by ongoing implementation and monitoring of improvements to privacy practices.
- Investment in appropriate security and privacy tools and technologies is required to create and sustain a privacy compliant environment.

# Actions Taken to Date

- **OSS has established a dedicated project team** to implement the recommendations of the Privacy Review and a **Privacy Action Plan** has been developed and approved.
- Work has been underway to **bridge outstanding gaps identified in PIAs**.
- Privacy and security **training is taking place on an ongoing** basis across the organization.
- Planning for **internal audit of key business lines that hold public personal information** before fiscal year end to measure progress made since review in 2005.
- An **internal privacy resource website** has been developed for OSS staff.
- **Active collaboration with the staff of the Office of the Chief Information** and the MGS Access and Privacy Office to assist with OPS wide privacy implementation strategies.

# OSS Progress

- **PKI certificate recovery has been upgraded** to a fully automated process (WebLRA) certified by Corporate Security, eliminating the need for manual intervention.
- **Directory of Records updated**, identifying personal information held.
- **Paperless pay cheques** have been implemented for over 64% of OPS employees.
- **Privacy related training** provided on an ongoing basis across OSS to ensure that all staff are aware of their roles and responsibilities.

# Where Are We Now?

- Today we have a measurable standard, based on “FIPPA Plus”, consistent with emerging privacy standards, and fair information practices.
- Our standard is a tool against which we will continue to measure ourselves. There is some interest in leveraging the OSS standard to create an OPS Privacy Standard.
- We have a clear understanding of where we are and where we need to be as far as privacy is concerned: where our business practices need to be strengthened, and where we are performing well. The guesswork has been taken out of privacy compliance.
- The review also identified best practices of privacy and protection in a horizontal organization where personal information is shared between business partners.
- Staff awareness has been raised through the exercise. There is more attention to privacy as a result of the review and training.

# Putting the Puzzle Together: A Roadmap

## First Steps:

- **Develop a Terms of Reference**
  - Scope: What are your business lines?
  - Deliverables: What reports do you want?
- **Form a Governance Structure**
  - Who can give direction and who needs to take ownership?
- **Outline an issues management protocol and process**
  - How to deal with issues as they arise.
- **Identify stakeholders and develop a stakeholder management strategy**
  - Error on the side of inclusivity

# A Privacy Compliance Roadmap



## Next Steps:

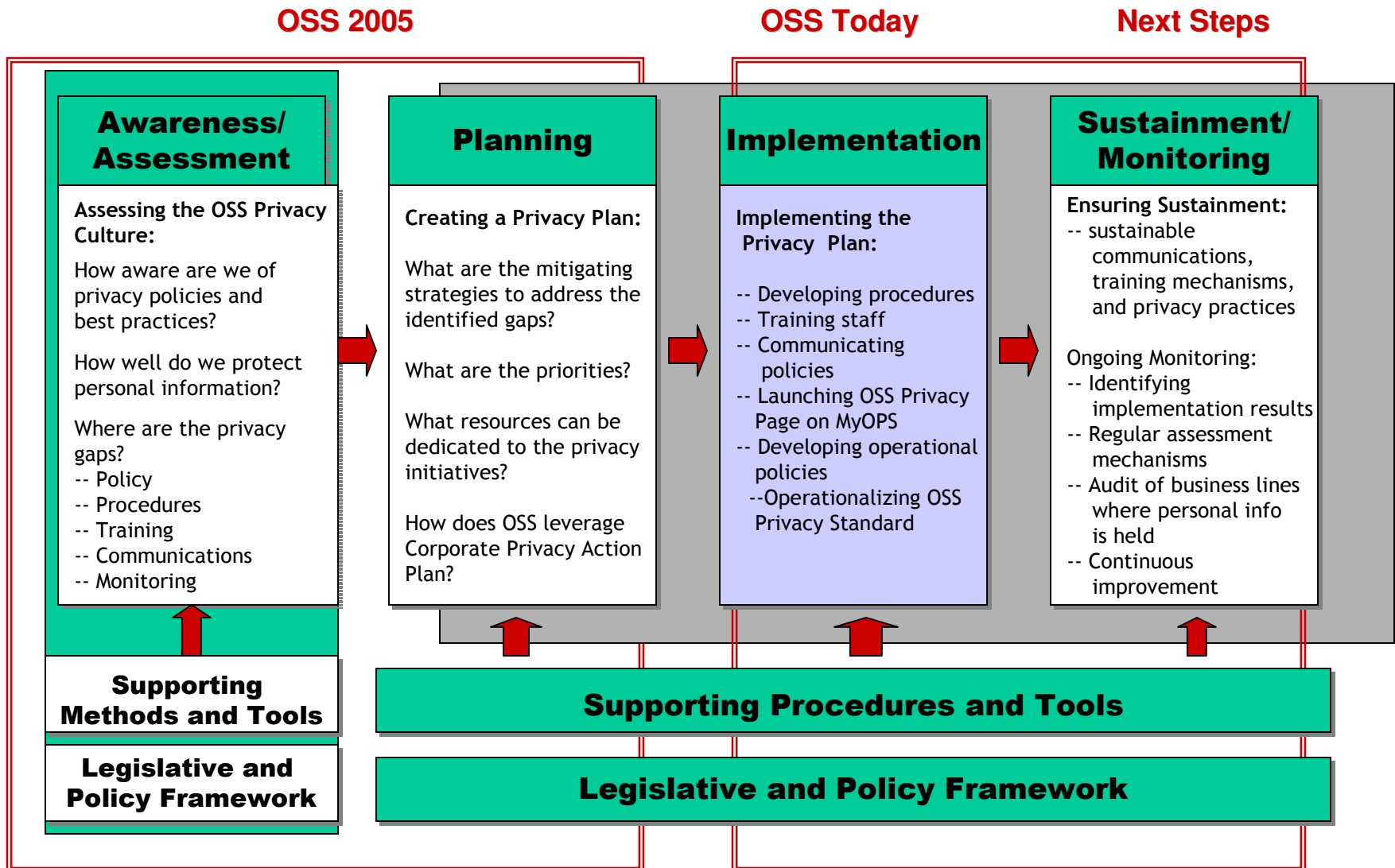
- Identify a standard against which you want your privacy practices assessed
  - Align with fair information practices
- Identify your holdings of personal information
  - Include PI you handle on behalf of others; or others handle on your behalf
- Identify your privacy policies, practices
  - PIAs, TRAs
  - Interviews
  - Other documentation
- Assess the gap between the privacy standard and your current policies and practices

# A Privacy Compliance Roadmap

## **Develop an action plan to address the gaps:**

- Communicate with others
- Develop policies where there are none
- Establish management and staff accountabilities
- Develop procedures
  - Fax protocol
  - Collection notices on documents
- Provide education and training
- Use tools and enablers
  - Privacy breach protocol
  - Standard as a self assessment tool
- Monitor progress and sustainment

# Building a Privacy Culture in OSS



# Where Can I Get More Information?

*If you have questions, please contact:*

➤ **Estella Cohen**, Manager  
OSS Privacy Review Implementation  
Project (416) 314-3959  
E-mail: [estella.cohen@mgs.gov.on.ca](mailto:estella.cohen@mgs.gov.on.ca)

➤ **David Jackson**, Privacy Advisor  
OSS Privacy Review Implementation  
Project (416) 325-1085  
E-mail: [david.jackson@mgs.gov.on.ca](mailto:david.jackson@mgs.gov.on.ca)

➤ *You can download a copy of the OSS Privacy Review report using this website address*

[http://www.mgs.gov.on.ca/english/releases/OSS\\_Summary\\_Report.pdf](http://www.mgs.gov.on.ca/english/releases/OSS_Summary_Report.pdf)