Privacy Impact Assessments at the National Capital Commission

The National Capital Commission (NCC) conducts privacy impact assessments to meet requirements under the *Privacy Act* and the Government of Canada's privacy standards and policies. Privacy impact assessments are

> "used to identify the potential privacy risks of new or redesigned federal government programs or services. They also help eliminate or reduce those risks to an acceptable level." (Office of the Privacy Commissioner website, <http://www.priv.gc.ca/fs-fi/02_05_d_33_e.cfm>, March 1, 2012)

When conducting privacy impact assessments, the NCC seeks

- to identify the data collected within a system that is subject to the *Privacy Act*;
- to evaluate the privacy issues related to the project; and
- to identify and manage the associated risks.

This document summarizes the findings in privacy impact assessments carried out by the NCC.

- Integrated Asset Management Information System
- Customer Relationship Management System
- Oracle Financials
- PeopleSoft
- LiveLink

Integrated Asset Management Information System

The NCC created the Integrated Asset Management Information System (IAMIS) to update and streamline the management of the NCC's moveable and non-moveable assets and agreements. Privacy issues were taken into account from the early stages of development. This greatly reduced the use of personal information about identifiable individuals within the system.

Personal Information

There is only one major data cluster in the Agreements Module that holds a significant amount of personal information. This is limited to only the most basic personal information required to perform necessary business functions.

Customer Relationship Management System

The Customer Relationship Management (CRM) system and related business processes are meant to improve the NCC's customer services and reduce risks for the organization. The system does this by tracking and managing contact information, incidents, issues, requests and feedback received from the public and interest groups.

A privacy impact assessment was conducted in the project's early stages so that privacy recommendations could be integrated into the design of the CRM system.

Privacy Recommendations

- Ensure that employees using the system have proper training in privacy policies and the handling of personal information.
- Conduct regular reviews of data management within the system.
- Have the NCC's personal information banks reflect how information is collected in the CRM system.
- Seek the review and advice of the Privacy Commissioner prior to implementing the system.
- Notify clients of data collection at the moment of collection (whether collected by phone, email, web or in person).
- Ensure that the system includes the necessary system security settings to ensure that personal information is protected in accordance with the *Privacy Act*.
- Ensure that the CRM system is designed and used in accordance with the NCC's policies on access to information and privacy.
- Use the NCC complaint process to handle complaints regarding personal information management .

Oracle Financials

The NCC uses the Oracle E-Business Suite Financials family of applications to automate and streamline its financial enterprise resource planning business processes. This software is complemented by an NCC-specific application called the Salary Management System. The Salary Management System is a custom application that resides within the Oracle Financials database, and was developed in-house by the NCC's information technology personnel.

Privacy Recommendations

- Audit Oracle regularly to ensure the correct implementation of the built-in security features permitting access and authorizations.
- Conduct continuous training at the NCC to remind staff of the sensitivity of personal data.
- Post the Oracle Financials privacy impact assessment summary on the NCC website.

PeopleSoft

The NCC uses Oracle's PeopleSoft as its human resource management software in order to manage human resources and compensation.

Privacy Recommendations

- Audit PeopleSoft regularly to ensure the correct implementation of the built-in security features permitting access and authorizations.
- Conduct continuous training at the NCC to remind staff of the sensitivity of personal data.
- Post the PeopleSoft privacy impact assessment summary on the NCC website.

LiveLink

LiveLink is the NCC's corporate document repository. It is used to store the NCC's electronic document records and to manage the NCC's inventory of hard copy documentation. While not intended to store personal information, the privacy impact analysis showed that there was a medium risk for personal information to be stored in LiveLink.

The greatest threat to LiveLink from a privacy perspective remains internal employees who e-file personal information from documents or emails (including attachments) inadvertently or incorrectly, with the resultant risk of unauthorized disclosure of sensitive personal information. Excessive trust is put upon the individual user in the absence of effective security awareness training and oversight on user actions. As such, the following measures are recommended to mitigate these risks.

Privacy Recommendations

- Consolidate and condense information security policies (including privacy protection requirements) and make them readily available to NCC employees.
- Establish an information security policies awareness program (including the protection of personal information) for new hires and provide the program annually thereafter to all employees.
- Conduct an audit of LiveLink to remove any sensitive and personal information that has been e-filed inadvertently. Conduct periodic audits afterwards to ensure compliance with the NCC policy on e-filing.
- Ensure that Human Resources Branch develops written procedures to reflect its current secure practices.
- Ensure that Human Resources Branch amends its current personnel forms used to collect personal information to include caveats informing individuals of the rights and obligations of all stakeholders regarding the protection of personal information.