Office 365 Privacy Impact Assessment Summary

Description of the Initiative

Moving to cloud services is a technology initiative being undertaken by the National Capital Commission (NCC), as the Government of Canada currently does not offer a cloud solution. Cloud services offer benefits that cannot be met within the NCC's current capacity and, in order to meet the expectations of Canadians, while providing reliable information services to NCC employees, the NCC must move toward more cost-effective, innovative and secure technological solutions.

This privacy impact assessment (PIA) has been prepared to assess the requirement surrounding the protection of personal information, including business sensitive information, when using cloud services. This report is meant to aid information technology, information management, and access to information and privacy staff, along with the directors and executive directors, to be better informed about the risks, and recommend appropriate safeguards in order to securely transition to the cloud.

This particular initiative focuses on transitioning the NCC's current Microsoft Office suite of products (Outlook, PowerPoint, Word and Excel) and our personal (P) network drive from on-premises storage to cloud storage. The solutions the NCC intends to leverage are Office 365 and OneDrive for Business, both of which are Microsoft products. The solution will leverage a "software as a service" (SaaS) model. The NCC is to be provisioned as a "tenant/subscriber," and Microsoft Canada, as the "service provider." NCC information will be stored and processed on data centres located in Canada and, as such, data sovereignty requirements should be satisfied.

The purpose of this initiative is to modernize NCC business and information technology (IT) processes. The many benefits of this initiative include the following, which are considered key:

- Leverage the security features inherent in cloud computing.
- Enable workforce mobility and ensure a high availability of services.
- Increase responsiveness.
- Reduce operational costs.
- Improve the NCC's disaster-recovery capabilities.
- Ensure quick access to innovative technologies.

Our initiative to move to the cloud involves the implementation of new software that supports the programs and activities of the NCC. This indicates that there is a potential for privacy concerns and risks. In order to ensure that the NCC is compliant with the *Privacy Act* and that privacy implications are identified, addressed and resolved, a decision was made to move forward with a PIA, prior to launching a pilot project.

Scope of This PIA

The scope of this PIA is centred on Microsoft Office 365 (cloud provider), a cloud-based SaaS collaboration and productivity suite. Within the scope will be the personal information data flows between NCC client subscribers (within the multi-tenant model) and Microsoft Cloud in addition to personal information stored within the data centres managed by Microsoft.

The suite offered by Microsoft consists of the following:

- Exchange Online
- OneDrive for Business
- Office Online (Word, Excel, PowerPoint)
- Backup to the Cloud
  Note: If the NCC decides to back up its data with a different service provider, then a new PIA will need to be performed.
- Skype for business online
  Note: If we deploy Skype for business, the recording feature will be disabled. If at any time the NCC wishes to enable the recording feature, we will review the impact on privacy, and prepare a new PIA, if required.
- SharePoint online (out of scope)

Assessment Objective

The objective of a PIA is to determine how a program or service, such as Microsoft Office 365, could affect the privacy of an individual. It can also aid in reducing possible negative effects on privacy that might result from a program or service. In addition, a PIA is a way for the NCC to state its commitment to protecting the privacy of individuals. PIAs promote transparency and accountability, and contribute to continued public confidence in the way that the NCC manages personal information. From a legislative perspective, the objective of this PIA is to identify areas of non-compliance with the *Privacy Act,* and determine how the NCC can avoid or minimize the loss, damage, misuse or abuse of personal information.

Risk Area Identification and Categorization

Risk level: 1 = low and 4 = very high

A. **Type of program or activity:** Administration of program or activity and services
   Level of risk: 2

B. **Type of personal information involved and context:** Sensitive personal information, including detailed profiles, allegations or suspicions, or particularly sensitive context surrounding the personal information
   Level of risk: 4

C. **Program or activity partners and private sector involvement:** Private sector organizations, international organizations or foreign governments
   Level of risk: 4

D. **Duration of the program or activity:** Long term
   Level of risk: 3

E. **Program population:** The program's use of personal information for external administrative purposes affects all individuals.
   Level of risk: 4

F. Technology and privacy

Does the new or substantially modified program or activity involve the implementation of a new electronic system or the use of a new application or software, including collaborative software (or groupware), to support the program or activity in terms of the creation, collection or handling of personal information? Yes.

Does the new or substantially modified program or activity require any modifications to IT legacy systems? Yes.

Does the new or substantially modified program or activity involve the implementation of new technologies or one or more of the following activities:

- **enhanced identification methods;**
- **surveillance; or**
- **automated personal information analysis, personal information matching and knowledge discovery techniques?** No.

G. Personal information transmission: The personal information is transmitted using wireless technologies.
Level of risk: 4

H. Potential risk that, in the event of a privacy break, there will be an impact on the individual or employees.

- Employees could access personal information and use or disclose it for personal purposes.
- A request may not actually be from a client (i.e. someone else may be using their email address).
- A client's personal information is compromised when transferred to the service provider.
- A client's personal information is compromised when transferred from the service provider.
- Inherent risks in sending personal information to a client via email.
- Inherent risks in storing personal information on cloud provider servers.
- Information stored on cloud provider servers inadvertently crosses international boundaries (data sovereignty violation).
- Accidental disclosure/leakage of personal information from one subscriber/tenant to another, which can happen in a multi-tenant cloud configuration.