Privacy Impact Assessment Summary: Gambit ID

INTRODUCTION

This privacy impact assessment (PIA) has been prepared to assess the requirements surrounding the protection of personal information when using Gambit ID. Gambit ID will be used by Corporate Security to capture security information on individuals (i.e. employees, students, volunteers, vendors, etc.) working with the National Capital Commission (NCC). It is also used to process security screenings electronically with external organizations such as the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS) for background investigations and final approvals. Gambit ID information will be stored electronically in Amazon data centres with a valid security certification in Montreal, Canada. All databases are physically or logically independent from other databases. Therefore, the solution has provisions in place to ensure that the NCC's data will not be disclosed to anyone outside the NCC. Personal information is protected under the *Privacy Act*, R.S.C. 1985, c. P-21.

In the context of this PIA, the project does not modify any other existing programs or activities, and all personal information collected and managed remains the same. Rather, the NCC is leveraging new technology to support these programs. A security assessment and authorization on Gambit ID and a review of our operational policies and procedures will allow us to assess risks related to the technical, physical, operational and legal safeguards of Gambit ID.

A privacy impact assessment was conducted to identify privacy issues and to provide strategies for mitigating the identified risks relating to the NCC's collection, use, retention and disclosure of personal information through Gambit ID.

BACKGROUND

The objective of this initiative is to enhance and align the security administration and screening process with the latest Government of Canada guidelines, while allowing more flexibility with a new cloud solution. Moving to cloud services is a technology initiative being undertaken by the NCC as the Government of Canada has instituted a cloud-first strategy. 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 towards more cost-effective, innovative and secure technological solutions.

DESCRIPTION AND SCOPE

This PIA has been prepared to assess the requirement surrounding the protection of personal information when using Gambit ID for NCC security screening, including criminal record checks, credit checks, employment checks, education checks and applicant record management in an individual aftercare information management module. Scope does not include processes and technology used by collaborators (RCMP and CSIS). Gambit ID is a cloud-based software as a service (SaaS) application that is hosted in a secured facility and maintained by Gambit ID. The NCC is to be provisioned as an "organizer" and Gambit ID as the "service provider."

Although Gambit ID offers various options, the NCC is using the modules that imitate the current processes for the security assessment process and fingerprinting (Gambit ID and Gambit ID Scan).

• The Gambit ID process provides workflows to process candidate security information which is filled in online. The process automates the creation of CSIS files, but the process for sending the files to CSIS remains the same: the files are attached to an encrypted email and sent to a secure mailbox. When the reply is received from CSIS, the results are uploaded to Gambit ID to continue the process.

• The Gambit ID Scan process collects the candidate's fingerprints, sends them to the RCMP with a secure process and receives the results. The security officer uploads the results into the Gambit ID system. There is no decision-making performed by the system. Any results must be reviewed and approved by the security officer.

Why the privacy impact assessment was necessary

A privacy impact assessment was needed to identify privacy issues and provide strategies for mitigating the identified risks relating to the NCC's collection, use, retention and disclosure of personal information.

Risk identification and categorization

The solution collects information through TBS and CSIS forms, including the new TBS 330-61, CSIS 4195 and 4160. The numbered risk scale is presented in an ascending order: the first level (1) represents the lowest level of potential risk for the risk area; the fourth level (4) represents the highest level of potential risk for the given risk area.

The initial step of the analysis consists of evaluating each risk area independently. The second step consists of grouping the individual results to determine if a more in-depth analysis is required. The greater the number of risk areas identified as level 3 or 4, the more likely it is that specific risk areas are needed to be addressed in a more comprehensive manner.

Types of personal information involved and context

The solution collects information through TBS and CSIS forms, including the new TBS 330-61, CSIS 4195 and 4160. This includes information on applicant names, addresses, family members, birthplace, gender, date of birth and work history. Additionally, the NCC security advisor may perform applicant education and employment checks depending on the situation or security screening level as the applicant proceeds through the security screening process, and also capture interview notes.

Personal information disclosure

Individuals are given the following information through the privacy statement: The information on the TBS screening form is required for the purpose of providing a security assessment. It is collected under the authority of subsection 7(1) of the *Financial Administration Act* and the Government Security Policy (GSP) of the Government of Canada and is protected by the provisions of the *Privacy Act* in institutions that are covered by the *Privacy Act*. Its collection is

mandatory for a CSIS background check. The information collected from the TBS screening form may be disclosed to the RCMP, which conducts the requisite checks and/or investigation in accordance with the Government Security Policy and entities outside the federal government (e.g. credit bureaus).

Data residency

Gambit ID is an Ottawa-based identity technology company with a cloud service production infrastructure hosted in Montreal, Canada. All databases are physically or logically independent from other databases. Their cloud-based solution is served through Transport Layer Security (TLS). TLS is the successor to Secure Sockets Layer (SSL) and is the industry standard for encrypting web content and protecting the integrity and privacy of data transferred from the servers to other computers.

Access and sharing of the data

Gambit ID has security controls and practices that are designed to protect the confidentiality, integrity and availability of customer content (NCC data) that is hosted on Amazon Web Services (AWS) and protect customer content from any unauthorized processing activities such as loss or unlawful destruction of data.

▪ Gambit ID employs measures designed to prevent unauthorized persons from gaining access to computing facilities in which customer (NCC) content is hosted.

▪ Gambit ID's access to customer content is restricted to authorized support staff on a need-to-know basis under a confidentiality agreement. There is no sharing of data outside of the boundaries of the system, unless explicitly requested by the NCC.

▪ Gambit ID can use strong passwords for user authentication. It stores passwords securely in an encrypted (AES256 data encryption) form.

▪ Amazon Web Services (AWS), which is the infrastructure as a service (IaaS) used for Gambit ID, does not have logical access to NCC information. Customer content on NCC's Gambit ID environment is logically or physically segregated from the content of other Gambit ID customers.

▪ Gambit ID respects customer privacy and is committed to protecting it by complying with policies. This policy is described in: https://www.gambitid.com/privacy.html.

The Gambit ID system is an enterprise-wide implementation. Information may be shared with other government departments, based on a specific need to identify, investigate and process applicants to their respective components. There is a secured connectivity with RCMP and CSIS for criminal and background checks. Therefore, the Gambit ID security screening results are shared with these departments by sending encrypted data files electronically.

File retention

The applicant form is kept for two years after the termination date, after which NCC Corporate Security will destroy the files. If the security screening is denied or revoked, the security screening file will be retained for at least 10 years after the employee's departure from the federal public service. The retention period can configure for different statuses in Gambit ID solution. The security officer can also search and export upcoming disposal files for information purpose.

Safeguards

Information is protected from misuse and unauthorized access through various administrative, technical and physical security measures. These controls are managed by the service provider, Gambit ID. Only NCC Corporate Security has "write" access to manage the screening process and selected human resources personnel have "ready-only" access to the aftercare management module based on a need-to-know basis to perform their job functions.

Technical controls: Technical security measures within the Gambit ID solution include restrictions to limit computer access to authorized individuals, required use of strong passwords for user authentication, and passwords that are stored securely in an encrypted (AES256 data encryption) format at rest and in transit.

Procedural controls: Regular review of Gambit ID security and operational procedures and best practices to enhance security are performed by a third-party auditor.

Privacy breaches

Ensuring that appropriate safeguards are in place to protect personal information is an ongoing process as security issues (administrative, physical and technical) evolve and change. The NCC follows the TBS Directive on Privacy Practices and, as such, has developed documented processes for privacy breach management.

Risk mitigation: Summary of the recommendations

1. Business authority must review and update PIA if significant changes occur with Gambit ID (process, information collected, new module, etc.).

2. Continuous monitoring (security in contracting) should be put in place to ensure Gambit ID cloud service and the NCC adheres to contractual arrangements and recommendations put forward.

3. Gambit ID should provide the NCC with certifications or demonstrate common security principles through the implementation of security controls that meet NCC criteria for security, availability, processing integrity and confidentiality/privacy principles. Certifications or attestations must be performed once every two years.

4. A security assessment and authorization should be performed to validate existing safeguards.

5. Gambit ID should demonstrate that they have updated incident response and management policies and protocols along with a reporting mechanism to inform the NCC of security and privacy breaches. Procedures must be in place to report breaches as soon as possible to the NCC, no later than five days after breach discovery.

6. Corporate Security staff training or guidance materials should include basic privacy protection notions.

7. The chief security officer should ensure that all employees accessing the systems have Access to Information and Privacy Fundamentals (I015) training whatever their status (students, contract employees, etc.). A training log should be kept, and a process should be in place to refresh knowledge once every three to five years.

8. The deprovisioning process should be documented and integrated with the NCC deprovisioning process.

9. Corporate Security must implement processes and ensure proper triggers to perform regular disposition.