Serving Government Website (2024)
System Description

Business Owner: **Francois Mollicone**
System Owner: **Mohamad Hamzeh**
Project Manager: **Abed Saab**
Security Practitioner: **Zeina Matta**

Security Lead: **Elena Taranu**
Security Assessor: **David O'Brien**

Date : **2024-07-05**
Version: **1.0**

Summary

Serving Government (https://service.ssc-spc.gc.ca is a Government of Canada Extranet web platform used to support SSC's Partners and clients and over 280,000 users.

The web platform is used exclusively by SSC partners to learn about SSC Services including email, networks, data centers, end-user IT and workplace technology devices. Serving Government is not accessible to members of the public.

Security Profile Summary The following table summarizes the Confidentiality, Integrity, and Availability ratings of Serving Government (SG) information assets required to determine the System Security Profile as assessed by IT Security, Corporate Services Branch.	
Confidentiality	The overall confidentiality rating is assessed as **Protected B**
Integrity	The overall integrity rating is assessed as **Medium**
Availability	The overall availability rating is assessed as **Low**
Security Profile	The system security profile is assessed as **PBML**

Approvals

System Description Completion- System Representative

As a System / Application business representative acting on behalf of the Program and Service Delivery Manager (PSDM), I have completed the System Description, including the Statement of Sensitivity (SoS) for your endorsement.

Completed by:

Francois Mollicone Signature:______________________________
Director, Digital and Multimedia Communications
Strategic Engagement Branch (SEB)
Shared Services Canada
613-290-8470; francois.mollicone@ssc-spc.gc.ca

System Description Validation- System Representative

As the System / Application business representative acting on behalf of the Program and Service Delivery Manager (PSDM), I have reviewed the System Description, including the Statement of Sensitivity (SoS) contained within and I affirm that the information is as complete and accurate as possible as of the date indicated.

Approved by:

Mohamad Hamzeh Signature: ______________________________
Director, Business Informatics Solutions
Chief Information Office
Enterprise IT Procurement and Corporate Services Branch
Shared Services Canada
613-410-2884; Mohamad.hamzeh@ssc-spc.gc.ca

IT Security Assessor Review

Reviewed by:

Steve Ross Signature: ______________________________
Manager
Corporate IT Security and Risk Management
Security Accommodations and Material Management (SAMM)
Enterprise IT Procurement and Corporate Services Branch (EITPCSB)
Shared Services Canada
613-218-8143; Steve.Ross@ssc-spc.gc.ca

Revision History

Each version of this document is identified in the following table, along with the reason for revision.

Version	Date	Reason for Revision	Modified By
0.1	2023-07-19	Initial Draft	Corporate IT Security
0.2	2023-07-27	Completed initial draft for SG	Business Informatics Solutions (Abed Saab)
0.3	2024-01-10	Completed statement of sensitivity	Business Informatics Solutions
0.4	2024-06-28	Add concept of operations related content	Business Informatics Solutions
0.5	2024-07-02	Applied new document template	Corporate IT Security
1.0	2024-07-05	Completed outstanding sections and final edits	Business Informatics Solutions

Table of Contents

1 Purpose of System Description

The System Description (SD) is the first security deliverable required as part of completing Security Assessment & Authorization (SA&A) of your system/service. The SD serves as a critical input to the selection of security controls (*i.e.*, Baseline Security Controls).

The SD consists of two (2) main portions, the first being the System Description where the final system/service is described in detail from multiple perspectives and the second portion being the Statement of Sensitivity (SoS) where the level of injury should a breach occur to the Confidentiality, Integrity and/or Availability (C,I &, A) is identified.

1.1 Key System Business Information

Project Parameter	Description
Business Owner	Name : Francois Mollicone Title: Director, Communications Directorate: Branch : Strategic Engagement Branch (SEB) Shared Services Canada Email : Francois.Mollicone@ssc-spc.gc.ca
Project Manager	Name : Abed Saab Title: Senior Project Manager, Serving Government Modernization, Business Informatics Solutions, Directorate: Chief Information Office Branch : Enterprise IT Procurement and Corporate Services Branch Shared Services Canada Email : abed.saab@ssc-spc.gc.ca

Project Parameter	Description
System Manager	Name : Nicholas Epifano Title: Manager, Business Applications, Business Informatics Solutions Directorate: Chief Information Office Branch : Enterprise IT Procurement and Corporate Services Branch Shared Services Canada Email : nic.epifano@ssc-spc.gc.ca *Note: As part of security Authorization, conditions and general terms must be adhered to. To ensure this occurs, security will require a single point of contact that will be responsible to ensure all required actions (including evidence) for each conditions of authorization is provided by the required date agreed upon within the systems Plan of Action & Milestones (PoAM). This individual would also be required to address and ensure alignment to the general terms of Authorization, specifically changes to the system and re-authorization.*
Security Assessment Authority	**Steve Ross** Manager, IT Security Risk and Policy Corporate IT Security Security, Accommodations and Material Management (SAMM) Enterprise IT Procurement and Corporate Services Branch (EITP-CSB) Shared Services Canada Steve.Ross@Canada.ca
Security Authorizer (Corporate)	**Sean Kealey** Chief Security Officer (CSO) Security, Accommodations and Material Management (SAMM) Enterprise IT Procurement and Corporate Services Branch (EITP-CSB) Shared Services Canada

Table 1 - Key Project Information

1.2 Security Assessment & Authorization (SA&A) Status

☐ The system is new, and/or has never been previously assessed & authorized.

If Yes, will any portion of the service/solution be outsourced?

☐ Yes. Outsourcing / issuing of a Contract will be required.

<If yes, provide additional details of the contracting activities here>

☐ No.

☒ The system exists and is undergoing a planned change. **Note:** The system/service changes will be described from an operational, technical and security perspectives below (Sections 3.3, 3.4 & 3.5).

☐ The current system/service Security Authorization is about to expire and re-assessment activities are required in order to maintain Authorization.

☒ Other (Please describe):

The current Serving Government website is comprised of a static website that serves fixed content to all its visitors. The website is available to all Government of Canada end user without the need to authenticate. The current information system is undergoing security assessment and authorization (SA&A) and the process is not yet completed.
The new Serving Government described in this document will entail the following changes and newly introduced features:

- Transition the website to the SSC 163enterprise Azure tenant;
- Add a restricted section requiring end user authentication and serving a small user-base of client department representatives (estimated at less than 1000);
- Add an end user authentication component which will leverage various GC Departments' Azure Active Directory (AAD) credentials;
- Add a reporting capability; and
- Upgrade the Content Management System (CMS) to Drupal 10.

2 System Description

This section provides a view of the information system which consists of data, processes, people, and technology from a business, technical, operation, and security perspectives. This allows for the security assessor to understand the manner in which the information system will be used, its components, dependencies and security requirements all required as part of the Security Assessment & Authorization (SA&A) process.

2.1 System Business Description

Serving Government (https://service.ssc-spc.gc.ca is a Government of Canada Extranet web platform used to support SSC's Partners and clients and over 280,000 users.

The web platform is used exclusively by SSC partners to learn about SSC Services including email, networks, data centers, end-user IT and workplace technology devices. Serving Government is not accessible to members of the public.

Based on consultations with SSC employees, partner departments and research, it was determined that the current Serving Government website is not adequately serving SSC clients or meeting the department's needs.

As outlined in our 2023–24 Departmental Plan, to offer a better service experience for clients, SSC launched an initiative to evaluate the possibility and impact of modernizing the Serving Government website by moving away from a static website (one-way information sharing) into an interactive portal.

The guiding vision for the future state Serving Government is a digital client hub that allows clients a seamless experience for learning about, and tracking SSC services. In addition, the modernized portal will speak with one SSC voice, providing a single source of truth for SSC services.

Transforming Serving Government into a digital client hub will help improve client satisfaction by providing more visibility into the SSC service delivery process and support SSC's service delivery capability and efficiency.

Based on an assessment of users and their needs, business requirements and design assumptions the technology options analysis recommended leveraging Drupal to build the interactive portal, which will rely on APIs published on the GC Enterprise Service bus to fetch information from downstream systems. The estimated user base for the new authenticated portion of the interactive website is approximately 1,000 users.

The static content and structure will largely remain the same. The Content Management System (CMS) will be Drupal 10 and will be hosted in the 163ent Azure tenet virtual machines (VMs).

The 163ent Azure tenet is supported by the SSC CSO (Cloud Service Operations) Branch which takes care of server provisioning, monitoring, incident detection, data backup etc.

2.2 Operational Environment

The system/service will be consuming Cloud services.

☒ Yes.

If Yes, select which cloud service model is applicable[1]:

□ Software as a service (SaaS)

☒ Platform as a service (PaaS)

☒ Infrastructure as a service (IaaS)

&

Select which cloud deployment model is applicable:

□ Public

□ Private

☒ Hybrid (i.e. combination of cloud deployments) – **The Serving Government platform relies on end user account provisioning and authentication provided by other government entities (i.e. relies on other distinct cloud infrastructures, service offered via other Department's tenants)**

□ Hybrid Cloud (i.e. combination of cloud deployment and on-premises.

□ No. The system/service will be administrated and operated solely on SSC premises (i.e. on-premises).

2.3 Operational Description

Serving Government (SG) is a website accessible within the Government of Canada network. It provides partners and clients, referred to in this document as "clients", with information on SSC's IT products and services. IT decision-makers and staff from client departments also frequent the website to learn about SSC plans and services and how they affect their department. This includes both the provisioning of services but also getting surrounding information on policies and plans.

The existing SG website operates as a static platform with one-way communication, primarily offering hyperlinks to various tools and information sources, resembling a one-stop shop. The goal of the SG modernization is to convert the current website into a dynamic client hub. This client hub will revolutionize the user experience by providing an interactive overview of key SSC interactions.

After the modernization process, the SG portal will consist of two primary components:

1. The "anonymous Component": This component will remain accessible to all users from various government departments, allowing them to browse the site and access information about SSC and its services. As part of the modernization, this component will be enhanced with additional functionalities to improve site navigation. Furthermore, the user interface will undergo a transformation to create a more user-friendly experience.

[1] For definitions of cloud deployments, reference CCCS - *ITSP.50.103* – Section 8.1.1, 8.1.2, & 8.1.3.

2. The "authenticated Component": This newly introduced component will be restricted to a specific subset of GC (Government of Canada) users. Access to this component will be granted only to users who have undergone pre-authorization through a defined business process. Once authorized, these users will be able to access the authenticated section of the portal.

The anonymous component of the site has an identical system description to the one provided for the Serving Government Drupal upgrade site. That component has an ongoing SA&A exercise that was targeting an ATO and go-live date of September 2023, and its assessment is yet ongoing.

The authenticated component will follow the following information patterns:

1. As a general rule, the information displayed to users would be fetched and displayed programmatically and "on the fly" as the user consumes the site. None of the data fetched would be store locally.
2. The portal will also rely on PowerBI reports that will be embedded into the authenticated component of the site, which will also entail showing data from the PowerBI platform that have been pre-designed to tackle some of the business requirements of the modernization. All data associated with this component will be fetched on the fly and none of it would be stored into the platform.
3. The authenticated site will also contain minimal new functionality, mainly building the Communications which will host tagged communiques available to all and various communications available only to the affected organizations.

Refer to the Serving Government Modernization Project's *Minimal Viable Product (MVP) High-Level Architecture* document for further details.

2.4 Additional Security Requirements

Business needs for security represent the authorizer's, business owner's, and other stakeholder's security requirements for the information system, defining in business terms the confidentiality, integrity and availability security objectives for each of the information system's business processes and related information holdings[2]:

- They are derived from laws, regulations, policies, directives, standards, contractual obligations, and objectives that govern business activities; and
- When supporting business activities, information systems need to satisfy the confidentiality, integrity, and availability needs of business activities through the implementation of appropriate IT security controls.

☐ Yes. The system/service has additional Business Needs for Security, they include the following:

- <Include Directive, Policy, Contractual obligation resulting in additional BSN above those listed in ***Annex D – Additional Business Needs for Security (BNS)***>

☒ No. The system / service does not have any additional BNS beyond those included in Annex D.

[2] Canadian Center for Cyber Security, Annex 2 - Information System Security Risk Management Activities (ITSG-33), Online, 2021, https://cyber.gc.ca/en/guidance/annex-2-information-system-security-risk-management-activities-itsg-33.

2.5 Technical Description

Below briefly describe the system/service from a technology point of view, similar to the information that would be contained within a Concept of Operations (ConOps) document. Descriptions and diagrams must address at a minimum, the following:

- Components of the system/services and where they reside (i.e. SSC enterprise data centre(s) (EDC) and/or specific cloud);
- System/Service dependencies and where they reside. Note: Dependencies are other system(s)/service(s) that your system/service is dependent on to function as intended;
- System Administrators & Users (including how they will Access & Authenticate to the system/service);
- System Interfaces (including internal & external interfaces);
- Data flows; and
- Use cases (if available).

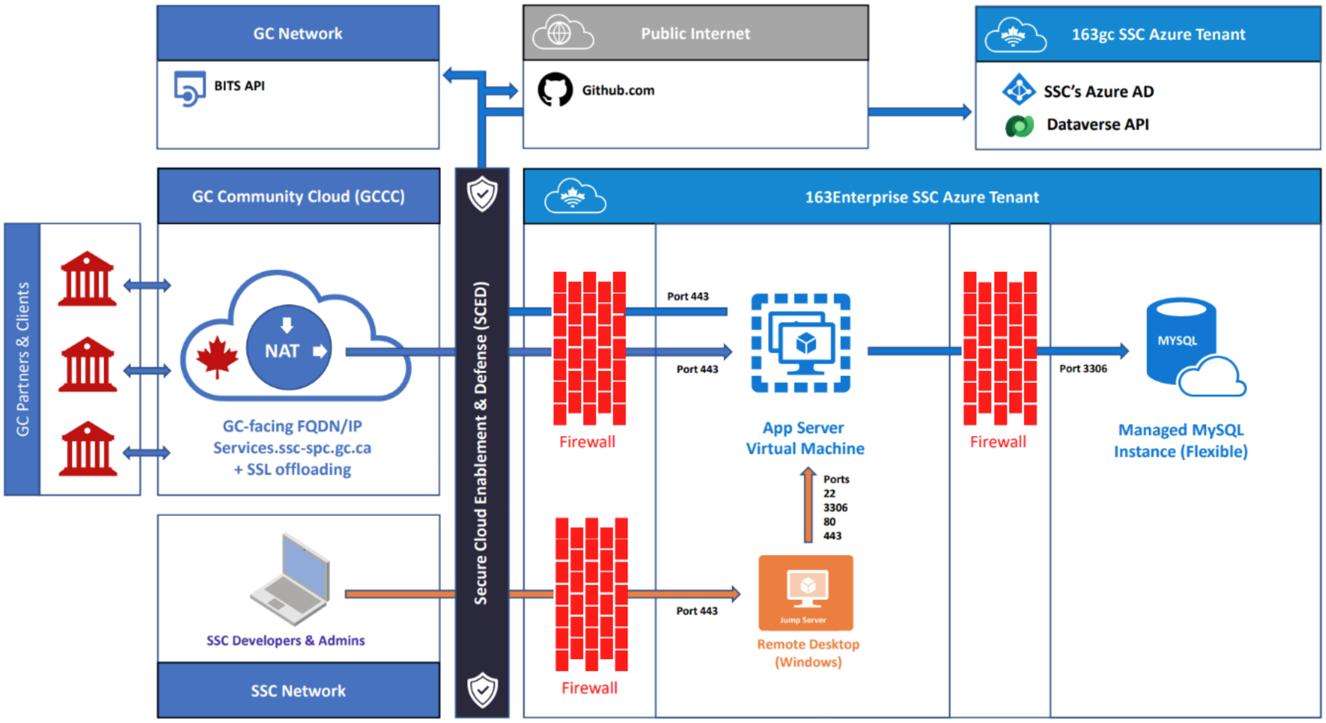

Figure 1 – Serving Government Physical Architecture Diagram

2.5.1 Users and Usage

User	Organization	Physical location	Usage
End User - Anonymous	End users on GC network	Anywhere, authenticated on GC network	Browse the static section of the SG site

End User – Internal users	Data Owners, Process Area Owners, Content Editors, Strategic Communications editors.	Anywhere, authenticated on SSC network	Browse the static and restricted sections of the SG site
End User – Authenticated clients and partners	Representatives from various SSC client and partner departments	Anywhere, authenticated on GC network	Browse the static and restricted sections of the SG site
Developer and application administrator	SEB/BIS application SMEs	Anywhere, authenticated on SSC network	Develop, deploy and maintain the solution applications (and platform?) i.e. Drupal, MySQL
Microsoft Azure administrator	SSC Cloud Service Operations team	Anywhere, authenticated on SSC network	Implement, monitor and maintain the Microsoft Azure tenet
Infrastructure administrator	SSC Engineering and Platform Support team	Anywhere, authenticated on SSC network	Maintain the network, platform, network devices and security devices
Analysts	SSC Engineering and Platform Support team	Anywhere, authenticated on SSC network	Monitor the applications performance, availability, security events, network, infrastructure and platform events

Refer to the Serving Government Modernization Project's *Minimal Viable Product (MVP) Functional Requirements* document, *Appendix C: Security Roles Requirements* for a breakdown of the application-level security roles.

Refer to the Serving Government Modernization Project's *Drupal Architecture* document for a description of the Drupal implementation of user roles and organizations.

2.5.2 Operating Environment

Cloud deployment model

Serving Government is deployed in a public cloud that is owned, managed and operated by the SSC Cloud Service Operations team.

Environments

An instance of the solution will be deployed in each of the following three environments, each hosted in the163 Enterprise SSC Microsoft Azure tenant:

- **Development Environment** – used for development purposes, available to the Serving Government's SSC developers and administrators
- **Test Environment** – used for testing changes and new releases of the website prior deployment into the production environment, available to the Serving Government's SSC developers and administrators. This environment will also be used by the Business Analyst to deliver demonstrations as necessary.
- **Production Environment** – the live site serving end users across various departments and agencies

Platform

Each instance of the solution will be comprised of the following technology stack:

- One VM hosting Drupal 10 and Apache

  As of June 12th Drupal version 10.2.5 with wxt version 5.2.2 (the latest) / Apache 2.4.52-1
- One VM hosting MySQL

Tools and cloud services

- **GitHub** – Code hosting platform for version control and collaboration, used as a repository of build artefacts.
- **GitLab** – Code hosting platform hosting Drupal code.
- **Composer –** Composer is a package management system that has one stop auditing of all dependencies (composer audit). Composer audit reports the latest CVE notices and facilitates updates. Composer is used to build the Serving Government application. When run, it indicates whether an update to any module is available and will identify the relevant CVE and packages involved.
- **Microsoft Entra ID (formerly Azure Active Directory [AAD])** – Leveraged to authenticate end users via their home department's AAD credentials.
- **Key Vault** – Azure service used for securely storing and accessing Serving Government platform secrets
- **Azure Common Endpoint** – Serves across all Microsoft Entra tenants, acting as a central hub that handles requests, used to authenticate Serving Government end users that are from a different tenant (i.e. from other Government Departments or Agencies).
- **Power BI** – Customer-facing reports, dashboards, and analytics embedded in the authenticated portion of the Serving Government portal.
- **Azure Monitor, Azure Application Insights, and Azure Log Analytics** – various Azure logging and monitoring services that will be configured to ingest Serving Government application event auditing logs to enable monitoring capabilities by the Engineering and Platform Support team.

Refer to the Serving Government Modernization Project's *Development Process* document for an overview of the Serving Government development tools and process description.

2.5.3 System Requirements

Refer to the Serving Government Modernization Project's *Minimal Viable Product (MVP) High-Level Architecture* document, for the Serving Government solution's environments and system requirements details.

2.5.4 Security Management

The SSC PBMM GC Cloud controls profile was tailored for applicability to the Serving Government platform. The resulting *Serving Government Security Controls Profile* was used as the baseline ITS requirements for this service. Additionally, service and application-specific security considerations have been documented in the Serving Government Modernization Project's *Minimal Viable Product (MVP) High-Level Architecture* document under the Security Considerations section.

Security of the Serving Government service is a responsibility shared among Microsoft, SSC CTO, SSC CIO, SSC SEB and SSC Corporate Security:

Microsoft – Microsoft has an inherent requirement to ensure security throughout the Azure cloud environment where access and visibility is very limited to the GC. As the cloud service provider, they are responsible for protecting the data centre from threats which include physical and environmental events; for protecting the physical network which includes hardware and cabling; for implementing any required Azure personnel security; and for providing cloud security services capabilities.

SSC Strategic Engagement Branch (SEB) – As the business owner SEB Communications is responsible for ensuring that the Serving Government service undergoes security assessment and authorization activities, authorizes connection from the Serving Government information system to other information system (i.e. EDR and use of other departments and agencies' AAD credentials) through the use of Interconnection Security Agreements such as the Client Credential Compliance Attestation letter. SEB is accountable for ensuring that the security posture of the service is maintained throughout its lifecycle.

SSC Chief Technology Office (CTO) – As the owner of the SSC 163enterprise cloud tenancy, the CTO Cloud Service Operations (CSO) team will be responsible for protecting the SSC network, and managing the network and security devices and services that are employed to protect it. CTO will be responsible for managing the GC client departments and agencies' access to the Serving Government website. They will also be managing firewall, Azure tenant level issues, and role-based access control (RBAC) for the infrastructure layer.

SSC Chief Information Office (CIO) – As the system owner, architect, developer, implementer and application maintenance provider, BIS is responsible for deploying and maintaining the website, provisioning access control to the application (Drupal), implementing adequate application-level event auditing, application-level configuration management, vulnerability management, patching and incident response, performing testing and flaw remediation, organization onboarding and related compliance/due diligence process.

SSC CIO Engineering and Platform Support (E&P Support) – Offering Infrastructure-as-a-Service and Platform-as-a-Service offerings to the Serving Government delivery team, the CIO E&P Support is responsible for defining platform baseline images, platform and database patching, platform and application monitoring capabilities, platform and database configuration management, performing server and data backups, ensuring the protection of audit event logs, detection and notification of cyber incidents, and implementing integrity checks throughout the CI/CD pipeline.

SSC Corporate Security – Responsible for personnel security, office physical security, and applicable departmental security policies and directives.

Refer to the completed version of the *Serving Government Security Controls Profile* for a full list of implemented security controls.

2.5.5 Access Management

Administrative access

Administrative access is restricted to the development and support teams using their Azure 163gc accounts, and enforces multi-factor authentication (MFA).

Network restrictions will control administrative access to the underlying solution infrastructure, and restrictions are applied to allow certain IP addresses.

Access is provided exclusively through a jump box and access to the jump box is tightly controlled through a process as follows:

➔ Access to the jump box is assigned through a webtop group and, for the Serving Government application, this group is managed and controlled by the CIO E&P Support team. One needs to submit the ticket in Jira or send an email to the CIO E&P Support team to request access to the jump box and application server.

In addition to the jump box, administrative access is controlled on the underlying virtual servers by providing access to the development and support staff (same process as above).

Administrative login events are audited, and access is provided based on roles (developer vs. app admin).

Developers & Infrastructure teams are having sudo access to application server.

Anonymous portion end user access

The anonymous portion of the website is accessible to all GC partners and clients i.e. end users who have been authorized onto the GC network.

Restricted portion of the website's end user access

Refer to the Serving Government Modernization Project's *Minimal Viable Product (MVP) High-Level Architecture* document, *Authentication and Authorization* section for further details regarding access to the restricted portion of the website.

Refer to the Serving Government Modernization Project's *Minimal Viable Product (MVP) Functional Requirements* document. See the *Portal Access Management* section for Access Management related functional requirements; as well as the *Appendix A: User Authentication & Authorization Process* for a depiction of the authentication and authorization process.

2.5.6 Security Monitoring

Monitoring of the Serving Government platform is a responsibility shared among the following entities:

Microsoft Azure – Microsoft has an inherent requirement to ensure security throughout the Azure cloud environment, although access and visibility will be very limited to the GC and to any of Microsoft's Azure clients. As the cloud service provider, they would be responsible for monitoring data centre related physical and environmental events, as well as the physical network which includes monitoring the hardware, cabling, capacity, etc.

SSC CTO Cloud Service Operations – As the owner of the SSC 163enterprise cloud tenancy, the SSC Cloud Service Operations team will be responsible for the monitoring of the SSC network, and network devices such as web application firewalls.

SSC Security Operations Centre (SECOPS) – The SECOPS team performs SSC network monitoring and will notify service owners of detected events that affect or impact their service.

SSC CIO Engineering and Platform Support – The CIO team responsible for the infrastructure and platform deployment, the Engineering and Platform Support team will be performing platform security monitoring including the virtual machines, operating systems and databases; as well as monitoring performance and other operating system related events such as security events (resources access activity, account management activity, etc.), capacity utilization thresholds, performance degradation, etc.

SSC CIO Business Informatics Services (BIS) – As the service designer, developer, implementor and operator, BIS will be responsible for ensuring that the application monitoring elements are in place. BIS will be configuring logging and monitoring requirements of application security events such as Drupal and its administrative command-line interface Drush file and configuration integrity, authorizations and resource access and account management activity, user authentication requests and responses, etc.

2.5.7 Training

End users will be provided with documented guidance on how to use the website's reporting features. At the present time, no further training is planned nor required.

Refer to the Serving Government Modernization Project's *User Guide*, for further details regarding end user training.

2.5.8 Maintenance

The various technical components of the solution will be maintained by CIO, according to its various teams' responsibilities as indicated in section *2.5.4 Security Management* above.

2.5.9 Reuse of previously approved solutions

The Serving Government platform will be deployed in the SSC 163Enterprise public cloud tenant which has previously been assessed by the SSC Security Management and Governance directorate.

To authenticate end users to the restricted section of the website, the platform will rely on the Azure Active Directory (AAD) services of each partner and client department to provide authentication of their respective end users.

3 Statement of Sensitivity

3.1 Confidentiality

The Policy on Government Security defines Confidentiality as "A characteristic applied to information to signify that it can only be disclosed to authorized individuals in order to prevent injury to national or other interests". Compromise occurs when an individual accesses information for which they have no authority or need-to-know.

3.1.1 Confidentiality Requirements

In the tables below, indicate the category and type of information that will be processed or stored by *Serving Government*. Please select all that applies.

Confidentiality Requirements		
Category	**Examples of Information Type**	**Percentage**
Unclassified or Public	□ Information available to the general public (e.g., approved and published policies, standards, tabled budgets) □ Information released for public awareness ☒ Other (please specify): Information available to GC entities (SSC partners and clients) such as information pertaining to the SSC service catalogue	50%
DESIGNATED (PROTECTED)	**Any information lying outside the national interest that could reasonably be expected to qualify for an exemption under one of the provisions of the *Privacy Act* and/or the *Access to Information Act* and applies to sensitive personal, private, and business information. *(See Annex A)***	
PROTECTED A (Compromise could result in limited injury.)	Personal information ☒ Individual's name □ Home address □ Home telephone □ Personal Record Identifier (PRI) □ Date of birth □ Letter of offer ☒ Individual's linguistic profile □ Contracts and tenders □ SIN ☒ Other (please specify): Information restricted to GC entities (SSC partners and clients), employee personal information such as work email address and	25%

Confidentiality Requirements		
Category	**Examples of Information Type**	**Percentage**
	phone number, role, news and communiqués, partner/client feedback.	
PROTECTED B (Compromise could result in grave injury, such as loss of reputation or competitive advantage.)	□ Information that contains an individual's social insurance number and an additional personal identifier, considered to be aggregate information such as name, address, and date of birth. □ Solicitor–client privileged information □ Criminal, medical, psychiatric or psychological records of individuals □ Trade secrets □ Information describing an individual's finances (e.g., income, assets, liabilities, net worth, bank balances), financial history or activities, or creditworthiness □ Personal recommendations or evaluations, character references or performance evaluations □ Information relating to the race, ethnic origin, colour, religious or political beliefs, including associations or lifestyle □ Treasury Board submissions, précis, memoranda to the President of the Treasury Board **unless** they contain information in the national interest, which must be categorized as classified □ Information whose unauthorized disclosure could result in: □ Substantial distress to individuals due to the loss of privacy □ Significant loss of competitive advantage to a Canadian company, third party, etc. □ Impeding the investigation of a serious crime □ Impeding the development of major government policies ☒ Other (please specify): authentication requests and response assertions; user credentials (for 2nd factor authentication), active and historical Business Requests, Change Requests, partner/client-specific reporting, ITSM data elements.	25%

Confidentiality Requirements

Category	Examples of Information Type	Percentage
PROTECTED C (Compromise of a very limited amount of information could result in exceptionally grave injury, such as loss of life.)	□ Information regarding the identity of government informants (witness protection program) □ Information whose unauthorized disclosure could result in: □ Extremely significant financial loss □ Loss of life □ Other (please specify):	0%
CLASSIFIED	**Any information related to the national interest that could reasonably be expected to qualify for an exemption under one of the provisions of the *Privacy Act* and/or the *Access to Information Act*. *(See Annex B)***	
CONFIDENTIAL (Unauthorized release could cause injury to the national interest.)	□ Information received in confidence from other governments or organizations □ International affairs and defence □ Information whose unauthorized disclosure could result in: □ Damage to diplomatic relations □ Damage to the operational effectiveness of the Canadian Forces □ Damage to the effectiveness of intelligence operations □ Other (please specify):	0%
SECRET (Unauthorized release could cause serious injury to the national interest.)	□ Information from investigations into activities that threaten national security □ Briefing notes for the Minister for Cabinet meetings, Cabinet papers (e.g., Memoranda to Cabinet, records of Cabinet decisions, committee reports) □ Details of discussions among Cabinet ministers on particular matters before Cabinet □ Treasury Board submissions, précis, memoranda to the President of the Treasury Board, information in the national interest □ Information whose unauthorized disclosure would result in: □ Increased international tension □ Serious damage to international or federal–provincial relations □ Serious damage to the operational effectiveness of the Canadian Forces □ Serious damage to valuable intelligence operations	0%

Confidentiality Requirements		
Category	**Examples of Information Type**	**Percentage**
	□ Significant threats to the national critical infrastructure □ Serious damage to civil order □ Other (please specify):	
TOP SECRET (Unauthorized release could cause extremely serious injury to the national interest.)	□ Information whose unauthorized release would result in: □ Widespread loss of life □ Loss of the continuity of government □ Damage to the effectiveness or security of Canadian and allied forces □ Damage to the effectiveness of valuable intelligence operations □ Damage to relations with other governments □ Severe long-term damage to the Canadian economy □ Other (please specify):	0%

Confidentiality Injury Test

Based on the table below, what would be the impact if the data or information associated with *Serving Government* was compromised? Check the applicable level in the table below.

(See Annex C for injury types and qualifiers)

Impact Type	**Very Low** (negligible/minor impact)	**Low** (minimal/limited impact)	**Medium** (moderate impact)	**High** (significant impact)	**Very High** (extreme/ irreparable impact)
Financial losses or economic hardship	☒ <$1,000	□ >$1,000	□ >$100,000	□ >$10 million	□ >$1 billion
Legal liabilities	☒	□	□	□	□
Loss of employment	☒	□	□	□	□
Loss of public trust or confidence in department	□	□	☒	□	□
Loss of service delivery or internal operations	☒	□	□	□	□
Harm to the safety and health of individuals	☒ (negligible discomfort or embarrassment)	□ (discomfort or minor embarrassment)	□ (injury, illness, public suspicion or doubt)	□ (potential loss of life, serious stress or trauma)	□ (widespread trauma and/or loss of life)

3.2 Integrity

Integrity is defined as "The state of being accurate, complete, authentic, and intact." Loss of integrity occurs when changes are made to information, processes or software that are unintended or unauthorized.

Integrity Requirements	
Will client organizations, programs or services depend on the accuracy of the information processed, stored or delivered by this system / application?	☐ No ☒ Yes (if yes, name the organizations, programs or services): Listed: https://service.ssc-spc.gc.ca/en/aboutus/partner-clients
What is the maximum acceptable data loss that can occur between the last point of recovery (e.g. last night's backup tape) and the point of system failure (e.g. system crash) in order to avoid critical business impacts as expressed in hours and/or days (known as (Recovery Point Objective or RPO)?	☐ No data lost – very high ☐ < 1 hour – high ☐ Between 1 hour and 1 day – medium ☒ Between 1 day and 5 days – low ☐ More than 5 days – very low
Is essential information available in other forms such as printed material or stored in other systems or applications?	☐ No ☒ Yes (if yes, please specify): The information is stored in GCDocs
Does any other government department or agencies hold duplicates of this information?	☒ No ☐ Yes (if yes, name the organizations, programs or services):
Do external organizations (other than Government) hold duplicates of this information?	☒ No ☐ Yes (if yes, name the organizations, programs or services):
Could the information be used in a court of law?	☒ No ☐ Yes

3.2.1 Integrity Injury Test

Integrity Injury Test

What would be the impact if the information processed, stored or delivered by *Serving Government* became corrupted, inaccurate, and incomplete or modified by an unauthorized user? Check the applicable level in the table below.

(See Annex C for injury types and qualifiers)

Impact Type	**Very Low** (negligible/minor impact)	**Low** (minimal/limited impact)	**Medium** (moderate impact)	**High** (significant impact)	**Very High** (extreme/irreparable impact)
Financial losses or economic hardship	☒ <$1,000	□ >$1,000	□ >$100,000	□ >$10 million	□ >$1 billion
Legal liabilities	☒	□	□	□	□
Loss of employment	☒	□	□	□	□
Loss of public trust or confidence in department	□	□	☒	□	□
Loss of service delivery or internal operations	☒	□	□	□	□
Harm to the safety and health of individuals	☒ (negligible discomfort or embarrassment)	□ (discomfort or minor embarrassment)	□ (injury, illness, public suspicion or doubt)	□ (potential loss of life, serious stress or trauma)	□ (widespread trauma and/or loss of life)

Has the system data ever been corrupted?

☐ Unknown.

☒ No.

☐ Yes. If yes, describe.

Has anyone ever accidentally deleted or modified system data?

☐ Unknown.

☒ No.

☐ Yes. If yes, describe.

3.3 Availability

The Policy on Government Security defines Availability as "The state of being accessible and usable in a timely and reliable manner." Loss of availability occurs when part or all of the system or the service provided by or information located in the system is unavailable when it is needed.

This section identifies both how long this system/service can be unavailable before there is a business impact and an injury occurs to an individual or to SSC. Note: Ensure to take in consideration and describe if the service/system availability requirements increase as a result of an increased injury occurring during specific period of time (i.e., years end, or tax time) if the system/service is not available.

Availability Requirements	
Does the system / application support a critical service[3]?	☒ No ☐ Yes (if yes, please specify):
Do employees depend solely on the system / application to perform their assigned tasks specific to the application?	☒ No (if no, please describe the other means or processes that are used, including manual processes): ☐ Yes
Are there any contractual obligations (contracts, service level agreements, etc.) that require the system / application to be available for specified periods of time?	☒ No ☐ Yes (if yes, please specify):
Are there any legislated obligations (laws, acts of Parliament etc.) that require the system / application to be available for specified periods of time?	☒ No ☐ Yes (if yes, please specify):
What are the regular business hours in which the system / application requires to be available (include consideration	☒ 7 days/week, 24 hours/day (continuous service required) ☐ 7 days/week, 8 hours/day (regular business hours) ☐ 5 days/week, 24 hours/day

[3] Critical service - A service whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, security or economic well-being of Canadians or to the effective functioning of the Government of Canada (GC).- *Policy on Government Security, Treasury Board Secretariat of Canada, 01 April 2012.*

for regional time zones where applicable)?	□ 5 days/week (weekdays), 8 hours/day (regular business hours) □ Other (please specify):
What is the maximum allowable downtime that the system / application can be unavailable before it poses a negative business impact on service delivery?	☒ 8 hours or less □ 1–2 days □ 3–5 days □ 6–14 days □ 15+ days
Does the level of impact for the client change during the business year? (For example downtime for the income tax remittal service would have a greater impact in March than in June)	☒ No □ Yes (if yes, please specify):
What is the maximum required restoration time (RTO) for the system before there is a significant impact on operations resulting in a high degree of injury to the health, safety, security, or economic well-being of Canadians? The maximum restoration time requirement should not exceed the highest level checked in the Availability Injury Test section below.	□ Continuous – very high □ Within 24 to 48 hours – high □ Within 3 to 10 calendar days – medium □ Within 11 to 30 calendar days – low ☒ More than 30 calendar days – very low
How long is system data required to be archived?	**2 years**

3.3.1 Availability Injury Test

Availability Injury Test

What would be the impact if *Serving Government* was unavailable beyond the maximum allowable downtime specified above? Check the applicable level in the table below.

(See Annex C for injury types and qualifiers)

Impact Type	**Very Low** (negligible/minor impact)	**Low** (minimal/limited impact)	**Medium** (moderate impact)	**High** (significant impact)	**Very High** (extreme/irreparable impact)
Financial losses or economic hardship	☒ <$1,000	□ >$1,000	□ >$100,000	□ >$10 million	□ >$1 billion
Legal liabilities	☒	□	□	□	□
Loss of employment	☒	□	□	□	□
Loss of public trust or confidence in department	□	☒	□	□	□
Loss of service delivery or internal operations	☒	□	□	□	□
Harm to the safety and health of individuals	☒ (negligible discomfort or embarrassment)	□ (discomfort or minor embarrassment)	□ (injury, illness, public suspicion or doubt)	□ (potential loss of life, serious stress or trauma)	□ (widespread trauma and/or loss of life)

Has the system ever been unexpectedly unavailable?

☐ Unknown.
☒ No.
☐ Yes. If yes, describe.

Is there a manual process (e.g. using paper forms) or other mechanism in place to continue operations if the system is unavailable (e.g. is there a way to provide the business function without the system)?

☒ No.
☐ Yes. If yes, briefly describe the manual process.

Do employees depend solely on the system to be able to perform their assigned tasks?

☒ No.
☐ Yes.

Are there any legal or contractual obligations (including SLA with other GC Departments/Agencies) that require the system to be available for specified periods of time?

☒ No.
☐ Yes. If yes, state the nature of the requirement.

Does a continuity plan exist to ensure the recovery of the system or provide the ability to operate manually in the event of a disaster (Business Continuity Plan, IT Continuity Plan, etc.)?

☒ No.
☐ Yes. If yes, explain.

Annex A – SSC Information Security Guide – Protected A, B, C

CATEGORY	PROTECTED		
DEFINITION	**ANY INFORMATION LYING OUTSIDE THE NATIONAL INTEREST THAT COULD REASONABLY BE EXPECTED TO QUALIFY FOR AN EXEMPTION UNDER ONE OF THE PROVISIONS OF THE *PRIVACY ACT* AND/OR THE *ACCESS TO INFORMATION ACT* AND APPLIES TO SENSITIVE PERSONAL, PRIVATE, AND BUSINESS INFORMATION.**		
SENSITIVITY	**PROTECTED A**	**PROTECTED B**	**PROTECTED C**
Definition	Compromise could result in limited injury.	Compromise could result in grave injury, such as loss of reputation or competitive advantage.	Compromise of a very limited amount of information could result in exceptionally grave injury, such as loss of life.
Examples	Routine correspondence with name, address, gender, race, date of birth or social insurance number or PRI *(Note: These data elements constitute Protected B information when compiled in an employee or client file)*	Personal, medical or financial matters *e.g. Treasury Board Submission, Personnel Screening Consent & Authorization, pay, test results, character references, conflicts of interest, eligibility for social benefits, etc.*	Threatening life and/or related to the Departments' operations *e.g. Investigations into threats to individuals*
Security Marking	Upper right corner on the face of the document		
Transmittal and Transport (Minimum Requirements) [1]	**NOTE:** When warranted by a Threat and Risk Assessment conducted by the CISO, use a higher security level of classification for storage, transportation and transmittal Refer to: **Security Organization and Administration Standard** of the PGS and Departmental Security		
By Hand	Between authorized persons only, depending on need-to-know principle	Between authorized persons only, depending on need-to-know principle	Between authorized persons only, depending on need-to-know principle
Mail/Courier [2] **(within and outside Canada)**	Single envelope, gum-sealed, with no security marking on the envelope	Double enveloped, gum-sealed, with no security marking on the outer envelope	Double enveloped, gum-sealed, with no security marking on the outer envelope A briefcase or other container of equal or greater strength, locked or sealed, can replace a single sealed envelope
Facsimile	Fax, electronic mail	Secure Fax	Secure Fax
Electronic Mail	Departmental network	Encrypt via ID-Based Certificate (myKEY)	Do not transmit
Electronic Storage	Departmental network	Encrypt via ID-Based Certificate (myKEY) or CISO Approved Encrypted USB Flash Drive	Consult CISO
Storage [3]	Locked cabinet	Monitored open shelving and Central Registry, locked cabinet and/or security container	Locked security container
Minimum Security Zone	Operation Zone	Operation Zone	Security Zone
Destruction [4]	RCMP Approved - Type III-A shredder	RCMP Approved - Type III-A shredder	RCMP Approved - Type II – Level 6 shredder
Personnel Screening Level	**Reliability Status**		

[1] **Transmittal - To send protected and classified information from one person or place to another by a third party. Transport – To physically hand carry protected and classified information from one person or place to another (Clarification through Security Office – RCMP Guide –G1-009). Approved by the Office of the Departmental Security Officer.**

[2] **Approved for the transportation of documents classified up to and including Secret** http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/list_0003_e.htm

[3] **Approved for the storage of records classified up to Secret in a Security or high Security Zone (4 door cabinet)** http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/equip_0343_e.htm

Approved for the storage of records classified up to and including Secret as described in the following link (DASCO) http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/equip_0373_e.htm

[4] **Suggested equipment for destruction of information up to and including Secret & Top Secret** http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/equip_0237_e.htm

Annex B – SSC Information Security Guide – Classified

CATEGORY	CLASSIFIED		
DEFINITION	ANY INFORMATION RELATED TO THE NATIONAL INTEREST THAT COULD REASONABLY BE EXPECTED TO QUALIFY FOR AN EXEMPTION UNDER ONE OF THE PROVISIONS OF THE *PRIVACY ACT* AND/OR THE *ACCESS TO INFORMATION ACT*		
SENSITIVITY	**CONFIDENTIAL**	**SECRET**	**TOP SECRET**
Definition	Unauthorized release could cause injury to the national interest.	Unauthorized release could cause serious injury to the national interest.	Unauthorized release could cause extremely serious injury to the national interest.
Examples	Records relating to ongoing consultations and negotiations between the Departments and their provincial counterparts	Minutes or records of discussion of Cabinet or Cabinet Committees relating to departmental responsibilities e.g. *Memoranda to Cabinet*	Information suspected of being a threat to the security of Canada *e.g. Terrorism*
Security Marking	Upper right corner on the face of the document	Upper right corner on each page Number each copy made Show the copy number on the face of each copy Maintain a distribution list	
Transmittal and Transport (Minimum Requirements) [1]	**NOTE:** When warranted by a Threat and Risk Assessment conducted by the CISO, use a higher security level of classification for storage, transportation and transmittal Refer to: **Security Organization and Administration Standard** of the PGS and Departmental Security		
By Hand	Between authorized persons only, depending on need-to-know principle	Between authorized persons only, depending on need-to-know principle	Between authorized persons only, depending on need-to-know principle
Mail/Courier [2] **(within and outside Canada)**	Double enveloped, gum-sealed, with no security marking on the outer envelope A briefcase or other container of equal or greater strength, locked or sealed, can replace a single sealed envelope	Double enveloped, gum-sealed, with no security marking on the outer envelope A briefcase or other container of equal or greater strength, locked or sealed, can replace a single sealed envelope	Consult CISO
Facsimile	Consult CISO	Consult CISO	Consult CISO
Electronic Mail	Do not transmit	Do not transmit	Do not transmit
Electronic Storage	Consult CISO	Consult CISO	Consult CISO
Storage [3]	RCMP approved, locked security container	RCMP approved, locked security container	RCMP approved, locked security container
Minimum Security Zone	Security Zone	Security Zone	High Security Zone
Destruction [4]	RCMP Approved - Type II – Level 6 shredder		
Personnel Screening Level	**Level I - Confidential**	**Level II - Secret**	**Level III - Top Secret**

[1] Transmittal - To send protected and classified information from one person or place to another by a third party. Transport – To physically hand carry protected and classified information from one person or place to another (Clarification through Security Office – RCMP Guide –G1-009). Approved by the Office of the Departmental Security Officer.

[2] Approved for the transportation of documents classified up to and including Secret http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/list_0003_e.htm

[3] Approved for the storage of records classified up to Secret in a Security or high Security Zone (4 door cabinet) http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/equip_0343_e.htm

Approved for the storage of records classified up to and including Secret as described in the following link (DASCO) http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/equip_0373_e.htm

[4] Suggested equipment for destruction of information up to and including Secret & Top Secret http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/equip_0237_e.htm

Annex C – Comparative Injury Types and Levels

Injury Type	Qualifier and Level				
	VERY LOW	**LOW**	**MEDIUM**	**HIGH**	**VERY HIGH**
Civil disorder or unrest	No reasonable or negligible expectation of injury	Civil disobedience or public obstructions	Riot	Sabotage affecting critical assets (e.g., critical infrastructure)	Large scale riot or sabotage requiring martial law
Physical harm to people	No reasonable or negligible expectation of injury	Physical discomfort or pain	Physical pain, injury, trauma, physical hardship or illness Serious discomfort or minor pain for over 1000 people	Physical disability, loss of life Physical pain, injury, trauma, physical hardship or illness for over 1000 people	Widespread loss of life
Psychological harm to people	No reasonable or negligible expectation of injury	Stress Serious inconvenience, minor embarrassment or minor doubts / uncertainty Minor inconvenience for over 1000 people	Distress or psychological trauma Serious embarrassment, doubts or uncertainty Public suspicion Serious inconvenience, minor embarrassment or minor doubts / uncertainty for over 1000 people	Mental disorder or illness, Serious stress / trauma. Serious embarrassment, doubts or uncertainty for over 1000 people. Widespread public suspicion Alienation of large groups	Widespread psychological trauma
Financial loss to individuals	No reasonable or negligible expectation of injury	Causing stress or discomfort	Affecting quality of life	Financial security compromised	
Financial loss to Canadian companies	No reasonable or negligible expectation of injury	Affecting performance	Reducing competitiveness	Viability compromised	
Financial loss to the Canadian government	No reasonable or negligible expectation of injury	Affecting program performance	Affecting program outcomes	Program viability compromised	Key programs viability compromised
Financial	$0 to $1k	$1k to $100k	$100k to $10M	$10M to $1B	Over $1 billion
Harm to Canadian economy			Affecting performance	Reducing international competitiveness	Compromising key economic sectors
Harm to Canada's reputation	No reasonable or negligible expectation of injury	Loss of Canadian public confidence	Embarrassment (home or abroad)	Damage to federal-provincial relations	Damage to diplomatic or international relations
Loss of Canadian sovereignty			Impediment to the development of major government policies	Impediments to effective law enforcement Loss of continuity of government	Loss of territorial sovereignty
Injury based on SSC Information Security Guide	**UNCLASSIFIED**	**PROTECTED A** Compromise could result in limited injury.	**PROTECTED B** Compromise could result in grave injury, such as loss of reputation or competitive advantage.	**PROTECTED C** Compromise of a very limited amount of information could result in exceptionally grave injury, such as loss of life.	

Injury Type	**Qualifier and Level**				
	VERY LOW	**LOW**	**MEDIUM**	**HIGH**	**VERY HIGH**
			CONFIDENTIAL Unauthorized release could cause injury to the national interest.	**SECRET** Unauthorized release could cause serious injury to the national interest.	**TOP SECRET** Unauthorized release could cause extremely serious injury to the national interest.

ANNEX D – Additional Business Needs for Security (BNS)

Justice Canada

- Access to Information Act;
- Privacy Act[4]; and
- Financial Administration Act.

Treasury Board Secretariat

- Policy on Service and Digital;
- Directive on Service and Digital;
- Policy on Government Security;
- Directive on Identity Management; and
- Directive on Security Management;

SSC

- Standard on Physical Security for Data Centres;
- Standard on the Management of Security Logs;
- Standard for Vulnerability Management;
- Security zone definition security standard;
- Supply Chain Integrity Standard;
- Perimeter Security Standard;
- Remote Access Security Hardening Standard;
- Endpoint Hardening Standard;
- Patch Management Standard;
- Server Hardening Configuration Standard;
- Logical Access Control Management Standard;
- Local Internet Access Services (LIAS) Standard;
- Network Access Control within the SSC Intranet Standard;
- Non-Person Entity Certificates for the SSC Intranet Standard; and
- Privilege Management Attributes Standard

[4] The system/service may has additional privacy requirements which could result in additional privacy activities that need to be completed outside of the SA&A process. For all SSC Privacy requirements, contact SSC ATIP @ (atip-aiprp@ssc-spc.gc.ca).