ANNEX 2, version 2.0

SECURITY AND PRIVACY

Table of Contents

1. SECURITY AND PRIVACY

This annex provides the security requirements that the e-Procurement Solution (EPS) will be required to implement. Following Contract Award, the Public Works and Government Services Canada (PWGSC) Security Assessment and Authorization (SA&A) process, as described in *section 6.6 PWGSC Security Assessment Authorization (SA&A) Process* of Annex 1 – Statement of Work, will assess how these requirements are addressed by the Contractor to assess compliance with Canada's security requirement.

If at any point during the SA&A process the Contractor cannot meet the security requirements described in *Section I – Security Requirements* to Canada's satisfaction, or if the security risks discovered through the SA&A process are deemed unacceptable by Canada, Canada, at its own discretion, may exercise any rights or remedies to which it is entitled under the Contract (including the right to terminate the Contract for default).

The GC has identified security controls to meet the Business IT Security Profile. The implementation of this set of controls by the Contractor must ensure GC information within the EPS is properly safeguarded to maintain a level of residual risk that is acceptable to Canada. Where Canada agrees, some of the security controls identified in *Section I – Security Requirements* below may be satisfied through existing industry standards, certifications and best practices.

As part of the SA&A process, if the security requirement are not met, corrective actions will be requested by Canada to address the concern. Canada may decide in its sole discretion whether it is satisfied that the remediation is adequate.

1.1 REMEDIATION(S)

Controls that are assessed as non-compliant during the SA&A process will be assessed by the Canada for risk exposure to the GC information. For risk item(s) that are assessed as unacceptable by Canada through the SA&A process, the Contractor must put in place adequate remediation to mitigate the risk(s) associated with the EPS.

1.2 OVERVIEW

This document consists of two sections:

1. Section I is a listing of the security requirements which have been categorized by the control families in Communications Security Establishment (CSE) Information Technology Security Guidance (ITSG)-33 (refer to https://www.cse-cst.gc.ca/en/node/265/html/22814 for more details on ITSG-33), as well as to the Government of Canada (GC) departmental and industry best practices. Throughout the life of the EPS, evidence of meeting the requirements will be assessed through the SA&A process.

2. Section II is a sample Security Requirements Traceability Matrix.

1.3 EPS IT SECURITY FOR SOFTWARE AS A SERVICE

The GC is moving to align with industry in adopting standards and best practices for sharing information. To assist in this initiative, the CSE has developed *The IT Security Risk Management: A Lifecycle Approach (as detailed within the CSE ITSG-33),* which provides the tools and guidance for GC organizations and contractors working on behalf of GC to ensure the risks to GC information systems are:

- identified;
- reported; and
- mitigated throughout a System Life Cycle (SLC).

Throughout the Term of this Contract, the need to protect GC information is of utmost importance and will be the driving force in determining the best method for securing the information assets.

The Business Needs for Security defines the business's targets for security, which are used to select the applicable controls from the CSE's ITSG-33 control catalogue based on the sensitivity, integrity and availability of the information.

1.4 SECURITY ASSESMENT AND AUTHORIZATION GATES

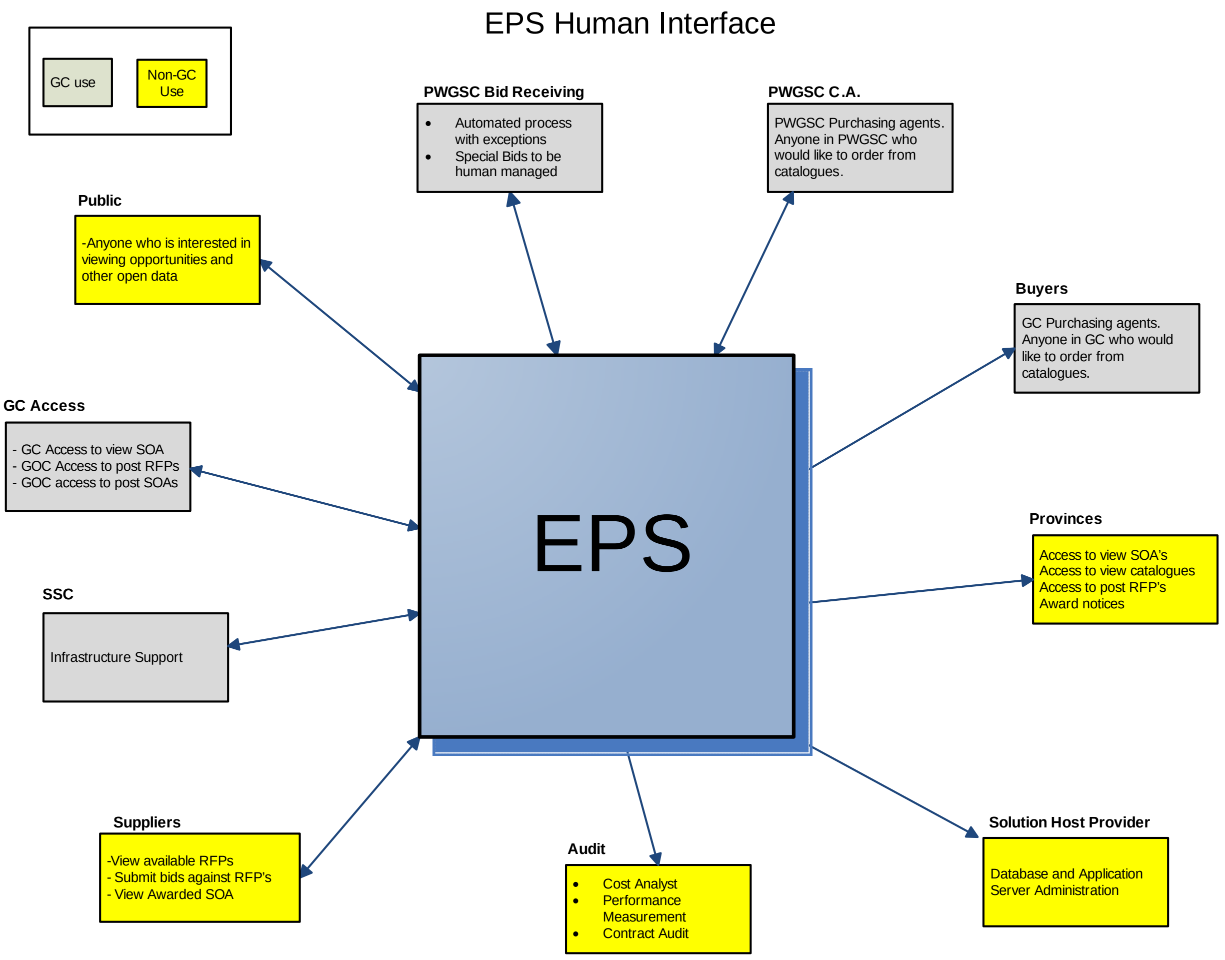
The SA&A process is based on secure System Development Lifecycle (SDLC). For the EPS, GC has identified three SA&A gates to ensure that the EPS is being designed, built, and integrated with security safeguards incorporated, thus providing a secure and stable EPS for GC. This is an iterative approach to the migration of the EPS from design and development to operational status. GC has outlined a set of deliverables expected at each gate. These deliverables will be reviewed and assessed, by GC, for compliance with the requirements identified in *Section I* of this annex. Furthermore, understanding that all areas of the SaaS may not be visible to GC, the Contractor must provide any Service Level Agreements (SLAs) or Memorandums of Understanding (MOUs) that may be in place, for GC's review, to facilitate a better understanding of the security posture of the EPS.

The Contractor must identify any industry standards or certifications they are compliant to in support of its EPS. The SAS 70 standard is one such standard which includes operating procedures for physical and perimeter security of data centers and service providers. Access, storage, and processing of sensitive data must be carefully controlled and is governed under standards such as ISO-27001, Sarbanes-Oxley Act [SOX], Gramm-Leach-Bliley Act [GLBA], Health Insurance Portability and Accountability Act [HIPAA] and industry standards like Payment Card Industry Data Security Standard [PCI-DSS].

1.5 BUSINESS CONTEXT

1.5.1 Business Use Cases

Figure 1 below provides an overview of the business use cases for the human interfaces associated with the EPS. It illustrates diversity of the user base for the EPS.


EPS Human Interface
GC use
Non-GC Use
PWGSC Bid Receiving
Automated process with exceptions
Special Bids to be human managed
PWGSC C.A.
PWGSC Purchasing agents. Anyone in PWGSC who would like to order from catalogues.
Public
-Anyone who is interested in viewing opportunities and other open data
Buyers
GC Purchasing agents. Anyone in GC who would like to order from catalogues.
GC Access
- GC Access to view SOA
- GOC Access to post RFPs
- GOC access to post SOAs
EPS
Provinces
Access to view SOA's
Access to view catalogues
Access to post RFP's
Award notices
SSC
Infrastructure Support
Suppliers
-View available RFPs
- Submit bids against RFP's
- View Awarded SOA
Audit
Cost Analyst
Performance Measurement
Contract Audit
Solution Host Provider
Database and Application Server Administration

1.6 TECHNICAL CONTEXT SUMMARY

The EPS must be a web-based Software as a Service (SaaS) solution that offers common procurement services for Government of Canada within and outside of the Government of Canada. The Technology Requirements for the EPS are defined in *Section 4.4 EPS Technology Requirements* of Annex 1 – Statement of Work.

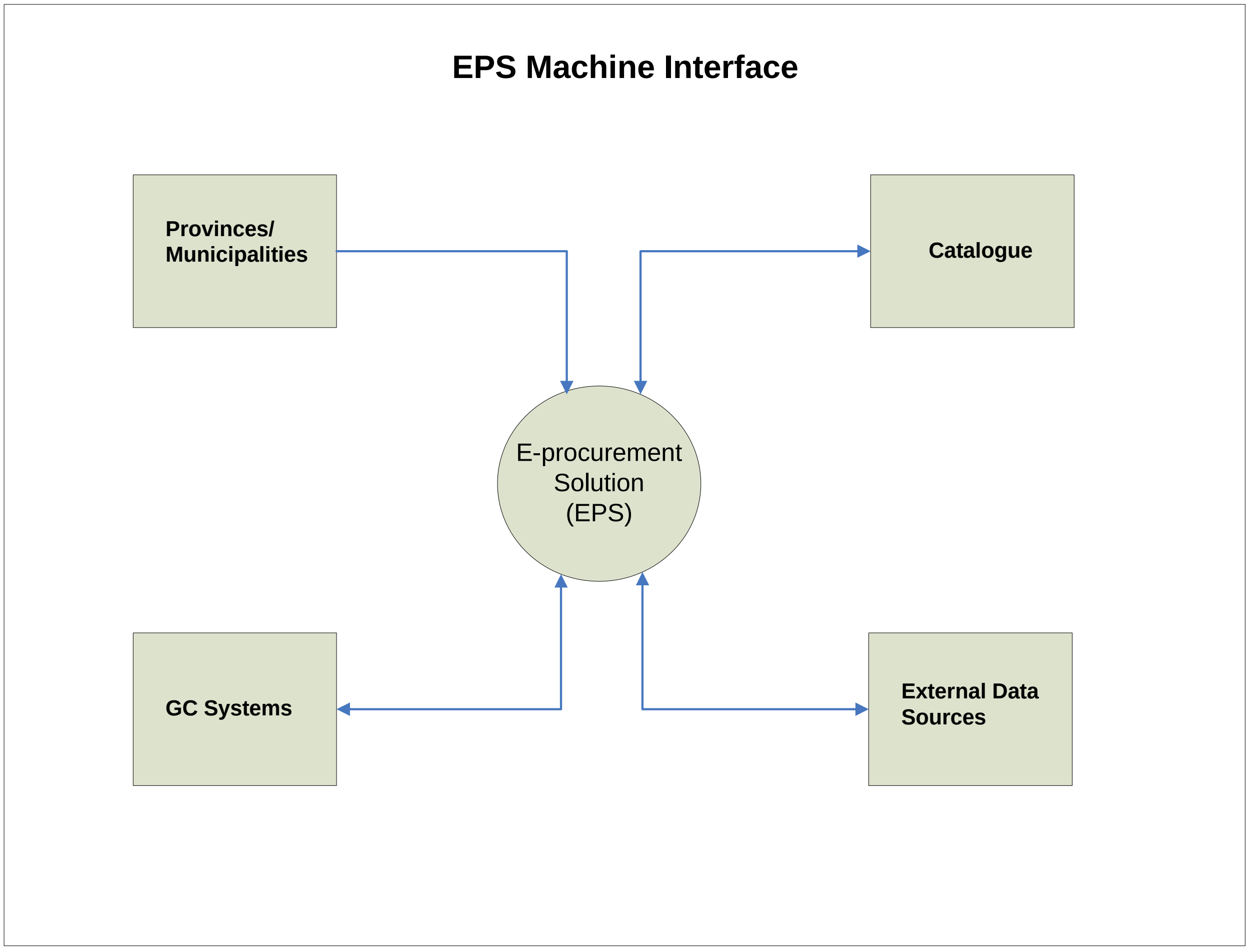
The EPS must be hosted as a cloud-based solution and the Contractor must ensure data segregation of the GC's data. The EPS is also required to securely exchange information with other support systems (both internal and external to GC) and back-office systems already in place, and those that will be introduced in the near future. For example the EPS is expected to play a key role in the GC's Procure-to-pay (P2P) process. While the overall P2P initiative is still in the planning stage, the EPS needs to be part of the overall business flow to support P2P.

The EPS must interoperate, through the Enterprise Service Bus (ESB) with the multiple GC installations of the SAP Department Financial and Materiel Management System (DFMS). The primary tool for interoperability between GC back office systems and business processes is the Oracle Enterprise Service Bus (ESB). The ESB is currently under development for the GC and is expected to be implemented in time for EPS implementation. For more details on the interoperability requirements for EPS see *Section 4.3 Interfaces with Government of Canada Systems* of Annex 1 – Statement of Work.

The EPS requires a secure access login via GC approved identity, credential and authentication management services in addition to secure access control to the various system components. *Section 4.5 Secure Access* of Annex 1 – Statement of Work provides more information on Secure Access requirements.

1.6.1 Machine Interface

Figure 2 below provides an overview of the machine interface associated with the EPS.



1.7 DESCRIPTIONS OF SECURITY POLICY AND PROCEDURE CONTROL CLASSES AND FAMILIES

The following provides a very high level description of the ITSG-33 security control catalogue which is organized into classes and control families. These controls families apply to the EPS security requirements and are addressed by the requirements listed in this annex. These control families are the basis of securing the application and data.

1.7.1 The technical security class consists of the following control families:

Access control: security controls that support the ability to permit or deny user access to resources within the information system;

Audit and accountability: security controls that support the ability to collect, analyze, and store audit records associated with user operations performed within the information system;

Identification and authentication: security controls that support the unique identification of users and the authentication of these users when attempting to access information system resources; and

System and communications protection: security controls that support the protection of the information system itself as well as communications with and within the information system.

1.7.2 The operational security class consists of the following control families:

Awareness and training: security controls that deal with the education of users with respect to the security of the information system;

Configuration management: security controls that support the management and control of all components of the information system (e.g., hardware, software, and configuration items);

Contingency planning: security controls that support the availability of the information system services in the event of component failure or disaster;

Incident response: security controls that support the detection, response, and reporting of security incidents within the information system;

Maintenance: security controls that support the maintenance of the information system to ensure its ongoing availability;

Media protection: security controls that support the protection of information system media (e.g., disks and tapes) throughout their life cycle;

Physical and environmental protection: security controls that support the control of physical access to an information system as well as the protection of the environmental ancillary equipment (i.e., power, air conditioning and wiring) used to support the operation of the information system;

Personnel security: security controls that support the procedures required to ensure that all personnel who have access to the information system have the required authorizations as well as the appropriate security screening levels; and

System and information integrity: security controls that support the protection of the integrity of the information system components and the data that it processes.

1.7.3 The management security class consists of the following control families:

Security assessment and authorization: security controls that deal with the security assessment and authorization of the information system;

Planning: security controls that deal with security planning activities including privacy impact assessments;

Risk assessment: security controls that deal with the conduct of risk assessments and vulnerability scanning; and

System and services acquisition: security controls that deal with the contracting of products and services required to support the implementation and operation of the information system.

SECTION I - SECURITY REQUIREMENTS

Table 1 below details the EPS security requirements.

EPS RFP ID	Requirement Category	Description
E2.1	Access Control	The Contractor must a) develop, disseminate, and review/update annually, the access control policies and associated access control requirements for EPS components; and b) provide GC with the operational security procedures that include operational roles and responsibilities for access control.
E2.2	Access Control	The Identity Credential and Access Management Service must automatically provision Accounts for EPS User Accounts and Generic Accounts, as follows: a) assign a unique EPS Account and Display Name in accordance with the standard defined in SOW, by applying configurable naming and conflict resolution rules; b) create an Account with no privileges; c) assign a one-time temporary password to the Account; d) assign Account attributes and security access privileges as specified by GC; and e) return the assigned EPS Account, Display Name, and one-time password to the Account Requester.
E2.3	Access Control	The Identity Credential and Access Management Service must a) prevent the re-use of an EPS Account as specified by GC; b) allow Account suspension policies as specified by GC; c) not allow access to a suspended Account; d) not allow an Account to send and receive EPS work flow messages if the Account is suspended; and e) not allow direct access to the EPS Solution Service for any Account, as specified by GC.
E2.4	Access Control	The Contractor must manage EPS Operators accounts by: a) identifying account types (i.e., individual, group, system, device, application, guest/anonymous, and temporary); b) establishing conditions for group membership; c) identifying authorized Operators of the EPS and specifying access privileges; d) requiring appropriate approvals for requests to establish accounts; e) selecting an identifier that uniquely identifies the Operator or device; f) assigning the Operator identifier to the intended party or the device identifier to the intended device; g) establishing, activating, modifying, disabling, and removing accounts; h) specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; i) notifying account administrator when temporary accounts are no longer required and when EPS Operators are terminated, transferred, or EPS usage or need-to-know/need-to-share changes; j) preventing reuse of identifiers for at least one year;

EPS RFP ID	Requirement Category	Description
		k) deactivating: i) temporary accounts that are no longer required; ii) accounts of terminated or transferred Operators; iii) accounts after a number of day of inactivity as specified by GC, and iv) temporary and emergency accounts over a given age; l) granting access to the e-Procurement Service based on: i) a valid access authorization; ii) intended system usage, and iii) other attributes as required by the Contractor or GC; m) reviewing accounts at least monthly; n) locking the account after ten (10) unsuccessful login attempts occurring within five (5) minutes, and o) keeping the account locked until manually unlocked by another Operator.
E2.5	Access Control	The EPS must log the following events: a) Account creation; b) Account modifications c) Account suspension; d) Account termination; e) Account deletion; and f) Account views of EPS accounts of which the User is not the primary owner.
E2.6	Access Control	The EPS must enforce access authorizations for Operators.
E2.7	Access Control	The EPS Data Loss Prevention (DLP) capability must a) detect violations of data loss prevention policies and apply response actions that include: i) blocking transfer of the transaction; ii) blocking transfer of the transaction and return a transaction to the Sender; and iii) other actions agreed to in writing between the Contractor and GC; b) allow real-time enforcement of data loss prevention policies based on the contents of the EPS transaction attributes including but not limited to i) strings, string patterns, and keywords within the transaction body; ii) file type of any attachments; and iii) specific domain(s) such as those known for malicious content.
E2.8	Access Control	The Contractor must implement separation of duties for Operators, as necessary, to prevent malevolent activity without collusion according to the role-based access profile assigned to the Operator.

EPS RFP ID	Requirement Category	Description
E2.9	Access Control	The Contractor must implement a least privileges policy for EPS Operators as follows: a) the access control mechanisms must be configured to implement least privilege, allowing only authorized accesses for Operators (and processes acting on their behalf) that are necessary to accomplish assigned tasks; b) create non-privileged accounts to be used for non-operations tasks; c) restrict authorization to super user accounts (e.g., root) to designated Operators; d) restrict sharing of Operator accounts; and e) must uniquely identify the human Operator who has performed each operation on the EPS.
E2.10	Access Control	The EPS must: 1. Display a logon banner approved by GC on the login page of any web-based application for Users. 2. include an access control mechanism that: a) prevents access to EPS components or resources without identification, authentication, and authorization; b) displays a GC-approved logon warning banner that authorized operators must acknowledge prior to being granted access to EPS components; c) notifies the operators, upon successful logon (access), of the date and time of the last logon (access), and d) uses a readily observable logout capability whenever authentication is used to gain access to EPS components. e) include an operator session lock mechanism that: i. prevents further access to components by automatically initiating an operator session lock after a period of inactivity no longer than 60 minutes; ii. prevents further access to components by initiating an operator session lock when requested by the operators; iii. displays a screen saver that contains no meaningful information to completely replace what was previously displayed on the screen upon activation of an operator session lock, and iv. unlocks an operator session after successful authentication of the operator.
E2.11	Access Control	The Contractor must ensure that any use of Remote Management within the EPS take place using a method approved by Canada that includes: a) Remote Management must be restricted to EPS located within a contractor Service Delivery Point using EPS dedicated management consoles; b) Documenting allowed methods of Remote Management and establish usage restrictions and implementation guidance for each allowed remote management method; c) monitoring for unauthorized Remote Management; d) authorizing Remote Management prior to connection; e) employing automated mechanisms to facilitate the monitoring and control of Remote Management methods; f) routing all Remote Management to EPS components through a limited number of managed access control points; g) protecting information about Remote Management mechanisms from unauthorized use and disclosure; and h) employing automated mechanisms to facilitate the monitoring and control of Remote Management methods.

EPS RFP ID	Requirement Category	Description
E2.12	Access Control	The Contractor must establish Policies and procedures, supporting business processes and technical measures, implemented within any environments supporting the EPS in order to protect EPS from wireless network environments, including the following: a) Perimeter firewalls implemented and configured to restrict unauthorized traffic b) Security settings enabled with strong encryption for authentication and transmission in compliance with CSE ITSB-111 for Protected 'B' data c) Security hardening by replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) d) User access including Operators to wireless network devices restricted to authorized personnel e) The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network.
E2.13	Access Control	The Contractor must implement a mobile device policy for EPS that includes the following at minimum a) Anti-malware awareness training, specific to mobile devices, must be included in the contractor's information security awareness training; b) A documented list of approved application stores has been defined as acceptable for mobile devices accessing or storing provider managed data; c) The contractor must have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store. d) If Applicable, the Bring Your Own Device (BYOD) policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage. e) The contractor must have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The contractor must post and communicate the policy and requirements through the company's security awareness and training program. f) All cloud-based services used by the Contractor's mobile devices or BYOD must be pre-approved for usage and the storage of eProcurement Solution GC business data. g) The contractor must have a documented application validation process to test for mobile device, operating system, and application compatibility issues. h) The BYOD policy must define the device and eligibility requirements to allow for BYOD usage. i) Contractor must keep and maintain an inventory of all mobile devices used by the Contractor to store and access e- Procurement Solution GC data. j) Contractor must include for each device in the inventory details of all changes to the status of these devices (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)). k) A centralized, mobile device management solution must be deployed to all mobile devices permitted to store, transmit, or process customer data.

EPS RFP ID	Requirement Category	Description
		l) The mobile device policy must require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices, and must be enforced through technology controls. m) The mobile device policy must prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) and must enforce the prohibition through detective and preventative controls on the device or through a centralized device management system (e.g., mobile device management). n) The BYOD policy, if applicable, must include clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy must clearly state the expectations regarding the loss of non GC eProcurement Solution business data in the case a wipe of the device is required. o) BYOD or contractor-owned devices are configured to require an automatic lockout screen, and the requirement must be enforced through technical controls. p) Changes to mobile device operating systems, patch levels, or applications must be managed through the contractor's change management processes. q) Password policies, applicable to mobile devices, must be documented and enforced through technical controls on all contractor devices or devices approved for BYOD usage, and must prohibit the changing of password/PIN lengths and authentication requirements. r) The mobile device policy must require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported). s) All mobile devices permitted for use through the contractor’s BYOD program or a company-assigned mobile device must allow for remote wipe by the contractor's corporate IT or must have all company-provided data wiped by the contractor's corporate IT. t) Mobile devices connecting to contractor networks, or storing and accessing company information, must allow for remote software version/patch validation. u) All mobile devices must have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel must be able to perform these updates remotely. v) The BYOD policy must clarify the systems and servers allowed for use or access on a BYOD-enabled device.
E2.14	Access Control	DELETED
E2.15	Access Control	The Contractor must limit the use of Contractor-controlled portable storage media within the EPS (e.g., thumb drive) as follows: a) restrict the use to authorized Operators only, and b) restrict the use to EPS components only.
E2.16	Security Awareness and Training	The Contractor must provide GC with the EPS operational security procedures that include operational roles and responsibilities for awareness and training.

EPS RFP ID	Requirement Category	Description
E2.17	Security Awareness and Training	The Contractor must provide security awareness and training for EPS Operators as follows: a) as part of initial training for new Operators; b) before authorizing access to the EPS or performing assigned duties, and c) annually or when security impacting changes to the EPS occur.
E2.18	Security Awareness and Training	The Contractor must monitor and document EPS security awareness and training for EPS Operators including: a) documenting who received what training course and when, and b) retaining records for the last three (3) years.
E2.19	Audit and Accountability	The Contractor must provide GC with the EPS operational security procedures that include operational roles and responsibilities for audit and accountability.
E2.20	Audit and Accountability	The EPS Identity Credential and Access Management Service must log the following events in accordance with the authentication event logging requirements for Level 3 Assurance, as detailed in ITSG-31 (https://www.cse-cst.gc.ca/en/node/267/html/22784). a) Successful authentication events; and b) unsuccessful authentication events.
E2.21	Audit and Accountability	The Contractor must a) review and update the list of auditable events for EPS at minimum once in 180 Business Days; b) include execution of privileged functions in the list of audit events; c) log events as identified and approved by GC; and d) automatically generate real-time alerts (e.g. using correlation rules) following indications of compromise or potential compromise.
E2.22	Audit and Accountability	The Contractor must ensure that the EPS: a) audits events such as unauthorized access to the EPS, unauthorized modification, changes to security attributes, privileged access to data fields, and b) produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event or audit events identified by type, location, or subject; and manages the content of audit records that are generated.
E2.23	Audit and Accountability	The Contractor must perform capacity management on the EPS audit record storage by: a) allocating enough audit record storage capacity; b) configuring auditing to prevent storage capacity being exceeded;

EPS RFP ID	Requirement Category	Description
		c) alerting the Operations Center when the allocated audit record storage volume reaches 75% of the audit record storage capacity; and d) overwriting the oldest audit records if storage reached maximum capacity.
E2.24	Audit and Accountability	The EPS audit function must respond to auditing failures by: a) alerting the Operations Center; and b) overwriting the oldest audit records if storage reached maximum capacity.
E2.25	Audit and Accountability	The EPS must use internal system clocks that are synchronized with an authoritative time source, approved by GC, to generate time stamps for audit records.
E2.26	Audit and Accountability	The EPS must: a) protect audit information from unauthorized access, modification, and deletion; and b) backup audit records onto a different system or media than the system being audited on a schedule as specified by GC.
E2.27	Security Assessment and Authorization	The Contractor must develop an EPS vulnerability mitigation plan, for approval by Canada, within five (5) Business Days of completion of a vulnerability assessment. The plan must include proposed protection measures to mitigate the risks identified from the vulnerability assessment.
E2.28	Configuration Management	The Contractor must develop, document, and maintain under configuration control, a current baseline configuration of the EPS components and the two (2) previous versions.
E2.29	Configuration Management	The Contractor must only allow authorized software, as documented by the Contractor and approved by Canada, to execute on the EPS.
E2.30	Configuration Management	The Contractor must a) plan, test the implementation of new and changed software, hardware and documentation for an EPS release not using the production environment or the Control Test Environment of the EPS; b) implement new and changed software, hardware and documentation for an EPS release as approved by Canada; and c) develop and implement procedures for the distribution, installation, and rollback of changes implemented for an EPS release.

EPS RFP ID	Requirement Category	Description
E2.31	Configuration Management	The Contractor must assess the security impact of changes by: a) analyzing new software before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice; b) informing GC of potential security impacts prior to change implementation, and c) checking the security functions, after changes are implemented, to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the applicable security requirements.
E2.32	Configuration Management	The Contractor must conduct audits of information system changes at least every 12 months and when indications so warrant determining whether unauthorized changes have occurred.
E2.33	Configuration Management	The Contractor must review EPS Operator privileges on an annual basis.
E2.34	Configuration Management	The Contractor must employ automated mechanisms to centrally manage, apply, and verify configuration settings and to respond to unauthorized configuration changes by creating a Security Incident Ticket.
E2.35	Configuration Management	The Contractor must open a security Incident Ticket when an unauthorized configuration change is detected in the EPS.
E2.36	Configuration Management	The Contractor must configure the EPS to provide only essential capabilities and specifically prohibits or restricts the use of functions, ports, protocols, or services as approved by Canada.
E2.37	Configuration Management	The Contractor must develop, document, and maintain an inventory of the EPS components that: a) accurately reflects their current configuration; b) is at the level of granularity deemed necessary for tracking and reporting; c) includes enough information to achieve effective property accountability; d) is available for review and audit by GC; and e) is updated as an integral part of component installations, removals, and EPS updates.

EPS RFP ID	Requirement Category	Description
E2.38	Configuration Management	The Contractor must provide an EPS configuration management plan that: a) addresses roles, responsibilities, and configuration management processes and procedures; b) defines the Configuration Items for EPS and when the Configuration Items are placed under configuration management; c) establishes the means for identifying Configuration Items throughout the system development life cycle and a process for managing the configuration of the Configuration Items; d) defines the processes for patch management on custom software utilized within the EPS that includes: I. identifying, reporting, and correcting flaws in custom software; II. testing software updates related to flaw remediation for effectiveness and potential side effects on the EPS before installation; e) iii) incorporating flaw remediation into the EPS configuration management process; f) defines the processes for patch management of the EPS components that includes: I. ensuring the latest version of applications and operating systems are used; II. ensuring that vulnerabilities are evaluated and vendor-supplied security patches are applied in a timely manner; III. prioritizing critical patches using a risk-based approach; IV. taking applications offline and bringing them back online; V. aligning criticality levels for patches as specified by GC; VI. rating of vulnerabilities against Common Vulnerabilities Scoring System (CVSS) v2; VII. testing and verification methodology to ensure that patches have been implemented properly; and VIII. notifying GC of configuration vulnerabilities that would allow an unauthorized individual to compromise the confidentiality, integrity, or availability of EPS.
E2.39	Configuration Management	The Contractor must provide GC with a EPS change management process that includes: a) Contractor's change management authorities; b) Contractor resource roles and responsibilities for change management; c) how The Contractor will use the change management process to support the development of the EPS (e.g., a concept of operation); d) method used to uniquely identify configuration items; e) configuration item identification method; and f) means for identifying Configuration Items throughout the system development life cycle and a process for managing the configuration of the Configuration Items.
E2.40	Contingency Planning	The Contractor must provide GC with the EPS operational security procedures that include operational roles and responsibilities for contingency planning.

EPS RFP ID	Requirement Category	Description
E2.41	Contingency Planning	The Contractor must work in conjunction with GC to establish national restoration priorities for EPS in an order of precedence as specified by GC.
E2.42	Contingency Planning	The Contractor must a) test the backup data for EPS monthly to verify media reliability and data integrity; and b) use a sample of backup data for EPS in the restoration of selected EPS functions as part of service continuity plan testing.
E2.43	Contingency Planning	The Contractor must store backup copies of operating system software, critical system software, and component inventory in a separate facility or fire-rated container that is not collocated with the EPS.
E2.44	Contingency Planning	The Contractor must restore the EPS to a known state after a disruption, compromise, or failure.
E2.45	Identification and Authentication	The Contractor must provide GC with the operational security procedures that includes operational roles and responsibilities for identification and authentication requirements specified in this SOW.
E2.46	Identification and Authentication	The EPS must a) uniquely identify and authenticate Operators (or processes acting on behalf of Operators). b) issue user name and password credentials for Accounts that comply with the requirements for Level 2 Assurance as described in ITSG-31 (https://www.cse-cst.gc.ca/en/node/267/html/22784). c) allow challenge/response questions for password recovery; d) allow one-time temporary passwords for enrolment and password recovery; e) allow one-time temporary passwords must be subject to a configurable validity period, as specified by GC; f) allow one-time temporary passwords must be sufficiently random so as to not be predictable as approved by GC; g) allow automatic advanced notification of pending password expiry as specified by GC; h) allow password recovery policies and processes; and i) authenticate all Software Client access to the EPS.
E2.47	Identification and Authentication	The EPS Identity Credential and Access Management Service must allow the binding and un-binding of one or more credentials to an individual Account. (e.g., an individual could use their EPS Level 2 credential to access the EPS as a User and use an additional X.509 credential to access the EPS for administrative functions.).
E2.48	Identification and Authentication	The EPS must a) enforce two-factor authentication using hard crypto token for all Operator accounts in compliance with CSE ITSG-31 (https://www.cse-cst.gc.ca/en/node/267/html/22784); and b) perform mutual authentication of Operators Portable Devices connected to the network and only accept authorized Operators Portable Devices.

EPS RFP ID	Requirement Category	Description
E2.49	Identification and Authentication	The Contractor must manage EPS Operators accounts by: a) identifying account types (i.e., individual, group, system, device, application, guest/anonymous, and temporary); b) establishing conditions for group membership; c) identifying authorized Operators of the EPS and specifying access privileges; d) requiring appropriate approvals for requests to establish accounts; e) selecting an identifier that uniquely identifies the Operator or device; f) assigning the Operator identifier to the intended party or the device identifier to the intended device; g) establishing, activating, modifying, disabling, and removing accounts; h) specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; i) notifying account administrator when temporary accounts are no longer required and when EPS Operators are terminated, transferred, or EPS usage or need-to-know/need-to-share changes; j) preventing reuse of identifiers for at least one year; k) deactivating: i) temporary accounts that are no longer required; ii) accounts of terminated or transferred Operators; iii) accounts after a number of day of inactivity as specified by GC, and iv) temporary and emergency accounts over a given age; l) granting access to the EPS based on: i) a valid access authorization; ii) intended system usage, and iii) other attributes as required by The Contractor or GC; m) reviewing accounts at least monthly; n) locking the account after 10 unsuccessful login attempts occurring within 5 minutes, and o) keeping the account locked until manually unlocked by another Operator.

E2.50	Identification and Authentication	The EPS Identification Credential and Access Management service must log the following events:
		a) account creation;
		b) account modifications
		c) account disabling,
		d) account termination;
		e) for Level 3 Assurance, as detailed in ITSG-31 (https://www.cse-cst.gc.ca/en/node/267/html/22784):
		i) password changes;
		ii) credential registrations;
		iii) password recovery;
		iv) expired credentials

EPS RFP ID	Requirement Category	Description
E2.51	Identification and Authentication	DELETED
E2.52	Identification and Authentication	The Contractor must manage user authenticators for Operators by: a) verifying, as part of the initial authenticator distribution, the identity of the individual receiving the authenticator; b) establishing initial authenticator content for authenticators defined by the Contractor; c) ensuring that authenticators have sufficient strength of mechanism for their intended use; d) establishing and implementing administrative procedures for initial authenticator distribution, lost/compromised or damaged authenticators, and revoking authenticators; e) changing default content of authenticators upon EPS component installation; f) establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g) changing/refreshing authenticators at a frequency not exceeding 180 days; h) protecting authenticator content from unauthorized disclosure and modification, and i) requiring Operators to take specific measures to safeguard authenticators.
E2.53	Identification and Authentication	The EPS must, for password-based authentication: a) enforce minimum password complexity of case sensitive, 15 characters, with at least one upper case, one lower case, one number, and one special character; b) encrypt passwords in storage and in transmission; c) enforce password maximum lifetime of 90 days, and d) prohibit password reuse for 10 generations.
E2.54	Identification and Authentication	The EPS Identity Credential and Access Management Service must provide a) the User with a checklist that presents the rules a password must comply with and check these rules positively as they are satisfied when the User enters the password. b) configurable User password rules as specified by GC that include: i) minimum number of total characters; ii) minimum number of uppercase and lowercase characters; ii) minimum number of numeric characters; iv) minimum number of non-alpha-numeric characters; v) words found in dictionary (English and French); vi) password re-use history; vii) maximum lifetime of the password.
E2.55	Identification and Authentication	The Contractor must require that the registration process for EPS Operators to receiver identifiers and authenticators be carried out in person before a designated registration authority with authorization by a designated Contractor's official (e.g., a supervisor).

EPS RFP ID	Requirement Category	Description
E2.56	Identification and Authentication	The EPS must not transmit clear text passwords over any network.
E2.57	Identification and Authentication	The Contractor must not allow unencrypted static authenticators to be embedded in EPS applications or access scripts or stored on function keys.
E2.58	Identification and Authentication	The EPS must obscure feedback of Operator authentication data (e.g., masking password fields) during the authentication process.
E2.59	Identification and Authentication	The Contractor must establish a process for maintenance personnel authorization that includes: a) maintaining a current list of authorized maintenance organizations or personnel; b) ensuring that personnel performing maintenance on the e-Procurement Solution have required access authorizations, and c) having designated personnel with required access authorizations supervising the maintenance activities when maintenance personnel do not possess the required access authorizations.
E2.60	Incident Response	The Contractor must a) provide GC with the operational security procedures that includes operational roles and responsibilities for Incident response requirements specified in this SOW. b) implement and test the service continuity plan (all processes, procedures, roles, responsibilities etc.) on an annual basis, and provide the test results to GC within 10 Federal Government Working Days of completion of the service continuity plan testing. c) provide a service continuity plan (SCP) to GC that includes: i. detailed plan and documented processes for restoring EPS; ii. details the communications plan with GC and its suppliers; iii. details plan and processes for transferring operational, management and administration functionality to a backup operations centre; iv. back up strategies for datacenter facilities, network facilities, operational support systems and data, and key service components; v. how The Contractor will ensure that its suppliers have in place service continuity plans; vi. describes the process for testing the Service Continuity Plan; vii. steps The Contractor will take if any of its key suppliers go out of business, and viii. steps The Contractor will take if any of its manufacturers or Original Equipment Manufacturers (OEM) is no longer considered a trusted manufacturer or OEM by GC.
E2.61	Incident Response	The Contractor must provide a final version of the Service Continuity Plan within 15 Federal Government Working Days after receiving comments from GC on the draft Service Continuity Plan.

EPS RFP ID	Requirement Category	Description
E2.62	Incident Response	The Contractor must implement the Service Continuity Plan (all processes, procedures, roles, responsibilities etc.), and any subsequent annual updates, within 60 Federal Government Working Days following acceptance by GC.
E2.63	Incident Response	The Contractor must provide to GC within 40 Federal Government Working Days of a request, evidence not greater than 12 months old, (e.g. test results, evaluations, and audits, etc.) that the Service Continuity Plan has been implemented correctly, operating as intended, and producing the desired outcomes in meeting GC's service continuity requirements.
E2.64	Incident Response	If The Contractor determines that it will take more than 40 Federal Government Working Days to provide the requested evidence for the Service Continuity Plan, The Contractor must notify Canada within 5 Federal Government Working Days of the original request for evidence, and request an extension, in writing with appropriate justification. Granting an extension is within Canada's sole discretion. Canada will accept certificate of compliance as evidence.
E2.65	Incident Response	The Contractor must respond to security alerts, advisories, and directives from designated external organizations, approved by GC, on an ongoing basis including: a) constantly monitoring security alerts, advisories, and directives; b) generating internal security alerts, advisories, and directives as deemed necessary or as directed by GC; c) disseminating security alerts, advisories, and directives to Operators with security responsibilities, and d) implementing security directives in accordance with established time frames, or notifies GC of the degree of non-compliance.
E2.66	Incident Response	In addition to any sources of intelligence on cyber threats and Incidents sources that The Contractor monitors in its routine operations, The Contractor must monitor cyber threats and incidents publications, from sources identified by GC (e.g. the Canadian Cyber Incident Response Centre (CCIRC) (http://www.publicsafety.gc.ca/prg/em/ccirc/anre-eng.aspx).
E2.67	Incident Response	The Contractor must provide a Security Operations Centre (SOC), prior to the completion of operational readiness phase, with the and resources required for the centralized monitoring and resolution (24 hours per day, 7 days per week, 365 days per year) of EPS Security Incidents.
E2.68	Incident Response	The Security Operations Center (SOC) must: a) Coordinate Security Incident response in close coordination with GC; b) include a unique and dedicated telephone number available 24 hours per day, 7 days per week, 365 days per year answered using the official language of Canada (French, English) as requested by the caller; c) act as a point of contact for communications with GC representatives for security incidents; d) not impact operations of EPS in case of a Contractor Security Operations Center (SOC) failure; e) notify GC within 15 minutes if Contractor SOC is not available and provide contact name GC can communicate as necessary during The Contractor SOC outage.

EPS RFP ID	Requirement Category	Description
E2.69	Incident Response	The SOC must work with GCs Information Protection Centre (IPC) for activities that include: a) integration of processes; b) oversight; c) security Incident handling and response; d) auditing; e) Security Incident containment, eradication and recovery that include: i. ability to dispatch the IT Security Incident Recovery Team (ITSIRT) to The Contractor site; and ii. allowing GC to provide on-site guidance and coordination.
E2.70	Incident Response	The Contractor must automatically provide Incident Ticket information by secure e-mail to a pre-defined distribution list for each EPS for Incidents where GC specifies: a) information from Incident Ticket; b) frequency of e-Procurement updates; c) distribution lists, and d) criteria for selecting Incidents (severity, priority, content of Incident Ticket).
E2.71	Incident Response	The Contractor must continue to automatically send secure e-mail upon updates of Incidents until the Incident is closed or GC cancels the automatic update reporting for the Incident.
E2.72	Incident Response	The Contractor must implement mitigation measures (e.g., firewall blocks, Intrusion Detection Prevention signatures, removing malicious malware) to contain a Security Incident, protect against cyber threats or address vulnerabilities.

E2.73	Incident Response	The Contractor must provide a Security Incident post-mortem report to GC, within 72 hours of a request by GC, that includes, but is not limited to:
		a) Security Incident number;
		b) Security Incident opened date;
		c) Security Incident closed date;
		d) description of Security Incident;
		e) scope of Security Incident;
		f) chain of events / timeline;
		g) actions taken by Contractor;
		h) lessons learned;
		i) limitations/issues with EPS, and
		j) recommendations to improve EPS.

EPS RFP ID	Requirement Category	Description
E2.74	Incident Response	The Contractor must monitor on a continuous basis events on the EPS to: a) detect attacks, Incidents and abnormal events against the EPS; b) identify unauthorized use and access of EPS Data and EPS components, and. c) respond, contain, and recover from threats and attacks against the EPS.
E2.75	Incident Response	The Contractor must provide training for EPS Operators in their security Incident response roles and responsibilities and provide annual refresher training.
E2.76	Incident Response	The Contractor must test the Incident response process for the EPS at least annually using comprehensive test scripts to determine the Incident response effectiveness including: a) documenting the test results; b) reviewing the test results with GC, and c) implement corrective actions as required by Canada within a timeframe agreed to with Canada.
E2.77	Incident Response	The Contractor must ensure that the security posture of the EPS is maintained by continuously: a) monitoring threats and vulnerabilities; b) monitoring for malicious activities and unauthorized access; and c) where required, taking proactive countermeasures, including taking both pre-emptive and response actions to mitigate threats.
E2.78	Incident Response	The SOC must a) accept e-mails from GC authorized representatives to a Contractor-provided mailbox with an auto reply to confirm receipt of the e-mail; b) acknowledge receipt of e-mails received from e-Procurement addresses authorized by Canada, within 15 minutes of receiving the e-mails 24 hours per day, 7 days per week, and 365 days per year; c) authenticate the identity of the requester using a process approved by Canada.
E2.79	Incident Response	The Contractor must create one or more Incident Tickets for each Incident it detects or reported by GC.
E2.80	Incident Response	The Contractor must physically and/or logically separate information that identifies and details Security Incidents from all other types of Incidents. Any security related investigation information generated as a part of the ticket must be recorded in GC dedicated storage.
E2.81	Incident Response	The Contractor must open an Incident Ticket within 5 minutes of notification for both Contractor-determined and GC-reported Incidents.

EPS RFP ID	Requirement Category	Description
E2.82	Incident Response	The Contractor must review lessons learned from ongoing Incident handling activities and implement resulting corrective measures to Incident response procedures, training, and testing/exercises.
E2.83	Incident Response	The Incident Tickets for Security Incidents must include, the following additional information: a) type and description of attack/event; b) whether attack appears to have been successful and impact; c) attack scope (to an organization or across many organizations); d) estimated number of systems affected by organization; e) list of systems affected by organization; f) apparent source/origin of attack/Incident/event; g) date/time of attack/Incident/event; h) estimated injury level /sector; i) estimated impact level; j) attack/Incident/event duration; k) actions taken; l) status of mitigations, and m) applicable logs or evidence data.
E2.84	Incident Response	The Contractor must report all suspected or actual privacy and security violations for EPS as Security Incidents.
E2.85	Incident Response	The Contractor must provide all evidence, in a COTS format specified by GC, associated to a Security Incident, within a time interval specified by GC that includes: a) results of historical logs and audit records research associated with one or many Partners based on criteria provided by GC; b) results of analysis of logs and audit records associated with one or many organizations based on criteria provided by GC; c) logs and audit records based on criteria provided by GC, and d) additional information or data as specified by GC.
E2.86	Incident Response	The Contractor must open an Incident Ticket within 5 minutes of notification for both Contractor-determined and GC-reported Incidents.
E2.87	Incident Response	The Contractor must update the Incident within 5 minutes of a change in status of a high priority Incident and within 15 minutes of a change in status of all other Incidents.

EPS RFP ID	Requirement Category	Description

E2.88	Incident Response	The Contractor's Incident Tickets must include and maintain, but not be limited to, the following dedicated information fields for all Incidents:
		a) Contractor's Ticket number;
		b) Incident description;
		c) Incident originator contact information (name, telephone number and e-Procurement address);
		d) Incident originator language;
		e) related Incident Tickets;
		f) date and time stamp when Incident Tickets initiated;
		g) date and time stamp when Incident Ticket closed;
		h) Incident Ticket type; type (e.g. production, functional testing, performance testing, security, etc.) as specified by GC;
		i) Incident Ticket severity;
		j) Incident Ticket impact;
		k) Incident Ticket priority;
		l) Incident Ticket status (i.e. open, closed, in progress, suspended, cancelled etc.);
		m) Incident Ticket escalations;
		n) GC's ticket number;
		o) Service functions impacted;
		p) affected Service Delivery Points;
		q) Contractor contact (name, telephone number and e-Procurement address);
		r) Partner identifier (If applicable);
		s) Interactions with third parties;
		t) activity log;
		u) root cause (if available);
		v) estimated time for resolution (updated every 15 minutes);
		w) resolution description and
		x) outage time (for closed tickets only).

E2.89	Incident Response	The Contractor must open an Incident Ticket within 5 minutes of notification for both Contractor-determined and GC-reported Incidents.
E2.90	Incident Response	The Contractor must update the Incident within 5 minutes of a change in status of a high priority Incident and within 15 minutes of a change in status of all other Incidents.

EPS RFP ID	Requirement Category	Description
E2.91	Incident Response	The Contractor must notify GC via phone and / or e-mail (7 days x 24 hours x 365 days), based on priority as specified by GC, of any suspected or actual Security Incidents, including but not limited to: a) ransomware attacks; b) denial of service attacks; c) malware; d) social engineering; e) unauthorized intrusion or access; f) information breach; and g) all other security breaches or cyber threats targeting GC.
E2.92	Incident Response	The Contractor must not withhold from Canada any information or data in its possession that relates to EPS or is associated with a Security Incident.

E2.93	Incident Response	The Contractor must provide a secure Security Management Portal that will allow GC to view security-related information within the EPS. This includes but is not limited to:
		a) security Incident reports, post-mortem, adhoc reports, and associated evidence;
		b) security Incident tickets;
		c) user activity reports;
		d) operator activity reports;
		e) access reports;
		f) configuration audit reports;
		g) configuration change reports;
		h) file integrity monitoring reports;
		i) inventory reports;
		j) vulnerability reports;
		k) configuration change reports;
		l) Emergency Request for Changes and Request for Changes;
		m) patches and security patches implemented;
		n) information on whether specific e-Procurements are being blocked/filtered and for how long; and
		o) other supporting documentation (e.g. whitelisting, blacklisting).

E2.94	Incident Response	The Contractor must report all suspected or actual privacy and security violations for EPS as Security Incidents.
E2.95	Incident Response	Meetings for Security Incidents, or security related matters as identified by GC, must be in Person in the National Capital Region (NCR) or via Teleconference during regular business hours (08:00 to 17:00 ET) Monday to Friday and during hours outside that time period as agreed to between the Contractor and GC.

EPS RFP ID	Requirement Category	Description
E2.96	Incident Response	The Contractor must be available to participate in a Security Incident briefing provided by GC, (e.g. for Classified briefing).
E2.97	Incident Response	The Contractor must have proper forensic procedures and safeguards in place that includes: a) the maintenance of a chain of custody for both the audit information, and b) the collection, retention, and presentation of evidence that demonstrate the integrity of the evidence.
E2.98	Incident Response	The Contractor must develop an incident response plan that includes: a) how The Contractor plans to identify, report, and escalate Security Incidents; b) a roadmap for implementing the Security Incident response capability that includes preparation, detection, analysis, containment and recovery; c) a description of the structure and organization of the Security Incident response capability; d) a high-level approach for how the Security Incident response capability fits into The Contractor's overall organization; e) a definition of reportable Security Incidents; f) a definition of metrics for measuring the Security Incident response capability; and g) a definition of resources and management support needed to effectively maintain and mature the Security Incident response capability.
E2.99	System Maintenance	The Contractor must perform controlled maintenance by: a) scheduling, performing, documenting, and reviewing records of maintenance and repairs on EPS components in accordance with manufacturer or vendor specifications; b) controlling all maintenance activities, whether performed on site or remotely, and whether the equipment is serviced on site or removed to another location; c) requiring that a designated Contractor's official explicitly approve the removal of the EPS components from The Contractor data centre for off-site maintenance or repairs; d) sanitizing equipment to remove all data from associated media prior to removal from Contractor's facilities for off-site maintenance or repairs, and e) checking all potentially impacted security requirements to verify that the controls are still functioning properly following maintenance or repair actions.
E2.100	System Maintenance	The Contractor must approve, control, monitor and maintain, on an ongoing basis, the hardware and software used for maintaining the EPS specifically for diagnostic and repair actions (e.g., a hardware or software tools that are introduced for the purpose of a particular maintenance activity).

EPS RFP ID	Requirement Category	Description
E2.101	System Maintenance	The Contractor must a) check all media containing diagnostic and test programs for malicious code before the media are used on EPS components; b) verifying that there is no EPS information contained on the equipment; c) sanitizing or destroying the EPS equipment; d) retaining the EPS equipment within the EPS facility or obtaining an exemption from a designated EPS Contracting Authority explicitly authorizing removal of the equipment from the EPS facility.
E2.102	System Maintenance	The Contractor must authorize, monitor, and control maintenance and diagnostic activities on the EPS by: a) allowing the use of maintenance and diagnostic tools approved by GC; (to be discussed) b) employing strong identification and authentication techniques in the establishment of maintenance and diagnostic sessions that tightly bound to the user and by separating the maintenance session from other network sessions with the EPS by either: (i) physically and/or logically separated communications paths; or (ii) logically separated communications paths using CSE-approved cryptographic modules and algorithms (see subsection Encryption Standards); c) recording maintenance and diagnostic sessions; and d) having designated personnel review the records of the maintenance and diagnostic sessions.
E2.103	System Maintenance	The Contractor must establish a process for maintenance personnel authorization that includes: a) maintaining a current list of authorized maintenance organizations or personnel; b) ensuring that personnel performing maintenance on the EPS have required access authorizations, and c) having designated personnel with required access authorizations supervising the maintenance activities when maintenance personnel do not possess the required access authorizations.
E2.104	Media Protection	The Contractor must provide GC with the operational security procedures that includes media protection requirements specified in this SOW.
E2.105	Media Protection	The Contractor a) must restrict access to IT media (digital and non-digital) containing EPS Data to authorized Operators; and b) employ mechanisms to audit access attempts and access granted.
E2.106	Media Protection	The Contractor must mark, in accordance with the provisions of the contract, removable IT media containing GC information indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.

EPS RFP ID	Requirement Category	Description
E2.107	Media Protection	The Contractor must physically and logically control and securely store IT media containing EPS Data in accordance with: a) Industry best practices; and b) GC approved equipment, techniques, and procedures for data destruction (either on or off-site), such as but not limited to: Storage • DASCO Secure PC, Fileserver, FAX Cabinets • Mobile Shelving, Security, TAB (to G1-028) • DASCO Information Storage Cabinets • Secur-File (2 and 4 drawer) - ACOPS 101 • Mobile Operations Security Safe - Type A & Type B Destruction service providers • Mobile Destruction Services - Iron Mountain (MDS-35-GTI); • Destruction Facility - RECALL (Toronto facility) • Destruction Facilities - Iron Mountain (Calgary) • Mobile Destruction Services - GigaBiter LLC • Destruction Facility - Absolute Data Destruction (Toronto) Paper Shredders • Dahle 20831 EC • Kobra 400 HS ES (400 HS AO ES) • HSM 411.2 HS • Roto 600HS • Fellowes HS-1010
E2.108	Media Protection	The Contractor must employ cryptographic mechanisms to protect information in storage that are approved by GC and are in compliance with CSE guidance (ITSG-111 https://www.cse-cst.gc.ca/en/node/1428/html/25015).
E2.109	Media Protection	The Contractor must sanitize and verify IT media containing EPS Data, both digital and non-digital, prior to disposal, release out of The Contractor's control, or release for reuse.

EPS RFP ID	Requirement Category	Description
E2.110	Media Protection	The Contractor must track, control and verify media sanitization by: a) performing media sanitization in compliance with ITSG-06 (https://www.cse-cst.gc.ca/en/node/270/html/10572) requirements for Protected B information; b) recording media sanitization actions; c) testing sanitization equipment and procedure to verify correct performance at least annually; and d) sanitizing re-allocated used storage devices prior to connecting them to the e-Procurement Solution.
E2.111	Physical and Environmental Protection	The Contractor must provide GC with the operational security procedures that includes physical and environmental protection requirements specified in this SOW.
E2.112	Physical and Environmental Protection	The Contractor must authorize, monitor, and control all components entering and exiting the EPS facilities and maintain records of those components and activities. Records must be made available monthly and as requested by GC.
E2.113	Physical and Environmental Protection	The Contractor must implement at alternate work sites management, operational, and technical security controls that achieve the same objectives as those implemented at the main EPS Facility. Alternate site(s) must be approved concurrently with the Primary sites by CISD/IISD.
E2.114	Personnel Security	The Contractor must, upon termination of an individual's employment associated with EPS: a) terminate physical access to EPS facilities for the employee; b) terminate EPS access, including remote access; c) retrieve all security-related property (e.g., employee identity card, physical authentication token); d) upon termination of individual employment, must conduct exit interviews; and e) upon termination of individual employment must retain access to organizational information and information systems in accordance with the TBS Personnel Security Standard.
E2.115	Personnel Security	The Contractor must have access agreements to the EPS or EPS Data where: a) prior to being granted access to the EPS or EPS Data, Operators sign an access agreement that list the formal sanctions process for failing to comply with the terms and conditions of the access agreement, and b) The Contractor reviews and updates access agreements to the EPS or EPS Data every two years.
E2.116	Personnel Security	The Contractor must a) prior to being granted access to the EPS or EPS Data, ensure that the Operators sign an access agreement that list the formal sanctions process for failing to comply with the terms and conditions of the access agreement, and b) provide training for EPS Operators in their responsibilities to protect the privacy and confidentiality of the EPS Data as per the terms and conditions of the EPS contract and in the sanctions for failure to comply. The Contractor must provide bi-annual refresher training.

EPS RFP ID	Requirement Category	Description
E2.117	Risk Assessment	The Contractor must provide a third party certified vulnerability test result with supporting RAW data within 10 Federal Government Working Days of a request by Canada, that includes: a) physical access to the EPS facilities (i.e. Contractor's facilities where the EPS (i.e. hardware and software) is located); b) network access(es) to the EPS to allow for authenticated and unauthenticated scanning of network components and security appliances, using GC and/or industry approved and acknowledged tools; c) assistance for the duration of any onsite portion of the vulnerability assessment of at least one technical resource that is familiar with the technical aspects of the EPS (i.e., the hardware, software, and network components, security appliances, and their configuration); and (d) Limiting GC Vulnerability Assessment to discovery and scanning activities to EPS and will not engage in disruptive or destructive activities.
E2.118	System and Services Acquisition	From the date vulnerabilities are formally identified, The Contractor must, at a minimum: a) Mitigate all high-risk vulnerabilities within 10 days; and b) Mitigate all moderate risk vulnerabilities within 30 days. c) Remediate all vulnerabilities within 30 days. Canada and Contractor will mutually agree and determine the risk rating of vulnerabilities.
E2.119	System and Services Acquisition	The Contractor must maintain the EPS's security authorization state through continuous monitoring and annual audit of the implemented security requirements within the e-Procurement Service to determine if the security requirements in the information system continue to be effective over time in light of changes that occur in the e-Procurement Solution and its operational environment.
E2.120	System and Services Acquisition	The Contractor must provide evidence to support authorization maintenance activities, within 30 days of a request by Canada, following all changes to the EPS within The Contractor's control.
E2.121	System and Services Acquisition	The Contractor must update, as requested by Canada, and within 30 days of a request by Canada, security operating procedures and demonstrate implementation as part of authorization maintenance.
E2.122	System and Communications Protection	The Contractor as part of the Security Operational Procedures must include policy and procedures to facilitate the implementation and maintenance of the system and communications protection requirements specified in this SOW and in applicable GC standards specified in this SOW.
E2.123	System and Communications Protection	The EPS must include controls to manage Denial of Service (DoS) attacks, in a manner that is consistent with leading industry practices, as agreed to by both GC and the Contractor, via the Security Assessment & Authorization (SA&A) process.

EPS RFP ID	Requirement Category	Description
E2.124	System and Communications Protection	1) The service design for EPS must conform to network security zoning in accordance with IT Security Guidance (ITSG) ITSG-22 (https://www.cse-cst.gc.ca/en/node/268/html/15236) and ITSG-38 (https://www.cse-cst.gc.ca/en/node/266/html/25034). Additionally, The EPS must monitor and control communications at the external boundary of the system and at key internal boundaries within the system in compliance with ITSG-22 (https://www.cse-cst.gc.ca/en/node/268/html/15236) and ITSG-38 (https://www.cse-cst.gc.ca/en/node/266/html/25034). 2) The EPS Contractor must monitor and analyze network traffic, in near real time, to detect attacks and evidence of compromised EPS components. 3) The EPS Contractor must detect attacks including but not limited to: a) ransomware attacks; b) denial of service attacks; c) malware; d) social engineering; e) unauthorized intrusion or access; f) information breach; and g) all other security breaches or cyber threats targeting GC.
E2.125	System and Communications Protection	The EPS must exclusively connect to external networks or information systems specified by Canada only through managed interfaces using boundary protection devices arranged in compliance ITSG-22 (https://www.cse-cst.gc.ca/en/node/268/html/15236) and ITSG-38 (https://www.cse-cst.gc.ca/en/node/266/html/25034).
E2.126	System and Communications Protection	The Contractor must actively manage all network connections to external services associated with the EPS as follows: a) deny all network traffic by default; b) define allowable traffic for each network connection (i.e. deny all, permit by exception); c) terminate the network connection associated with a communications session at the end of the session or after a configurable number of minutes of inactivity specified by GC; d) document each exception to the traffic flow policy with a supporting need and duration of that need; e) review exceptions to the traffic flow policy at least annually; f) remove traffic flow policy exceptions that are no longer supported by an explicit business need; g) monitor traffic for unusual or unauthorized activities or conditions; and h) as necessary, monitor traffic at selected interior points within the system (e.g., subnets, subsystems) to discover anomalies.
E2.127	System and Communications Protection	The Contractor must prevent Contractor managed devices (e.g.: notebook or other device used for administration) that are connected with the EPS from communicating outside of that communications path (e.g. accessing the Internet via a separate connection available to the device).

EPS RFP ID	Requirement Category	Description
E2.128	System and Communications Protection	The EPS must detect extrusion events as soon as possible and Canada must be notified upon detection.
E2.129	System and Communications Protection	The Contractor must monitor and analyze hosts behaviours (Host-based Intrusion Detection and Prevention) to detect attacks and evidence of compromised hosts as soon as possible and notify Canada.
E2.130	System and Communications Protection	DELETED
E2.131	System and Communications Protection	The Contractor must configure boundary protections (i.e. firewall) to fail safe (i.e. no traffic goes through) upon failure.
E2.132	System and Communications Protection	The EPS Design a) must allow mutual authentication of connections, between the EPS and other domains as specified by Canada, and exclusively exchange information with these other domains using mutual authentication. b) Must ensure that the integrity and confidentiality of EPS Data during transmission and at rest is protected using cryptographic solutions unless otherwise protected by alternative mechanisms approved by Canada.
E2.133	System and Communications Protection	The EPS must protect the integrity and confidentiality of EPS Data during transmission and at rest using Communications Security Establishment -approved cryptographic modules and algorithms (see subsection Encryption Standards), unless otherwise protected by alternative physical measures approved by Canada.
E2.134	System and Communications Protection	DELETED

EPS RFP ID	Requirement Category	Description
E2.135	System and Communications Protection	The EPS Design must ensure that a) cryptographic solutions (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable) in use for EPS: i) use cryptographic algorithms and cryptographic key sizes and crypto periods that have been approved by CSE and validated by the Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/), and are specified in ITSB-111 (https://www.cse-cst.gc.ca/en/node/1428/html/25015) or in a subsequent version; ii) be implemented in a Cryptographic Module, validated by the Cryptographic Module Validation Program (https://www.cse-cst.gc.ca/en/group-groupe/crypto-module-validation-program) to at least FIPS 140-2 validation at Level 1, and iii) operate in FIPS Mode. b) the integrity and confidentiality of EPS Data during transmission and at rest is protected using cryptographic solutions unless otherwise protected by alternative mechanisms approved by Canada.
E2.136	System and Communications Protection	The Contractor must not prohibit a User to encrypt, decrypt, sign and verify EPS attachment files using Certificates trusted by the GC.
E2.137	System and Communications Protection	The Contractor must only allow pre-approved mobile code in the EPS thus denying any other mobile code from being downloaded and executed.
E2.138	System and Communications Protection	The EPS component or components that collectively provide name/address resolution service for the EPS must implement internal/external role separation.
E2.139	System and Communications Protection	The EPS must allow the authentication of all types of Software Clients with a EPS credential.
E2.140	System and Communications Protection	The EPS must protect the integrity and confidentiality of EPS Data during transmission and at rest using Communications Security Establishment -approved cryptographic modules and algorithms (see subsection Encryption Standards) unless otherwise protected by alternative physical measures approved by Canada.

EPS RFP ID	Requirement Category	Description
E2.141	System and Communications Protection	The Contractor, at their discretion, can use non-dedicated hardware, non-dedicated software for the operation, administration and management of EPS Management Data. Any use of non-dedicated hardware, non-dedicated software is only allowed for EPS Management Data according to the following conditions: a) must not access, process or store EPS User Data; b) must not access, process or store EPS System Data; c) must not access, process or store user account names and passwords; d) must be logically segregated from other client's data; e) must adhere to all EPS requirements outlined in Annex 2 Security Requirements; f) must not access, process or store information labeled as Protected or Classified unless approved in writing by Canada; g) must not access, process or store service design information for the EPS; and h) must not allow for the control or modification of the dedicated EPS.
E2.142	System and Communications Protection	The EPS must include dedicated controls for any network interconnections between dedicated and non-dedicated EPS, according to the approved Security Design, that includes: a) boundary protection whereby, the Contractor must use current or previously evaluated physical firewall appliances (http://www.cse-cst.gc.ca/its-sti/services/cc/index-eng.html) validated under a recognized Common Criteria scheme against an approved Protection Profile that considers firewall evaluation. The Contractor must obtain approval from Canada for alternative physical firewall appliances;; b) incorporation of Contractor provided threat detection/prevention solutions; c) routing of traffic through authenticated proxy servers; and d) role based access control with least privilege.
E2.143	System and Communications Protection	The Contractor must physically and/or logically separate a) information that identifies and details Security Incidents from all other types of Incidents. Any security related investigation information generated as a part of the ticket must be recorded in GC dedicated storage; b) ensure that any network configuration details contained in any asset records and configuration records management systems for the EPS are encrypted.; c) the network IP traffic of the EPS System Data from all other EPS Data; and d) logically separate the network IP traffic between the EPS Management Data and the EPS User Data.
E2.144	System and Communications Protection	The categorization of data for EPS as either EPS System Data, EPS User Data or EPS Management Data will be at the sole discretion of GC and based on comparison to other similar data.
E2.145	System and Information Integrity	The Contractor must provide GC with the EPS operational security procedures that includes operational roles and responsibilities for system and information integrity requirements specified in this SOW.

EPS RFP ID	Requirement Category	Description
E2.146	System and Information Integrity	The Contractor must define and execute the processes for patch management for the EPS components that includes: a) ensuring the latest version of applications and operating systems are used; b) ensuring that vulnerabilities are evaluated and vendor-supplied security patches are applied in a timely manner; c) prioritizing critical patches using a risk-based approach; d) taking applications offline and bringing them back online; e) aligning criticality levels for patches as specified by GC; f) rating of vulnerabilities against Common Vulnerabilities Scoring System (CVSS) v2; and g) testing and verification methodology to ensure that patches have been implemented properly. h) defines the processes for patch management on custom software utilized within the EPS that includes: i) identifying, reporting, and correcting flaws in custom software; ii) testing software updates related to flaw remediation for effectiveness and potential side effects on the EPS before installation; and iii) incorporating flaw remediation into the EPS configuration management process.
E2.147	System and Information Integrity	The Contractor must a) centrally manage the malicious code protection mechanisms; b) automatically updates malicious code protection/malware mechanisms (including signature definitions) within 6 hours of availability and as requested by GC; c) prevents non-privileged users from circumventing malicious code protection capabilities; d) updates malicious code protection mechanisms only when directed by a privileged user; and e) does not allow users to introduce removable media into the EPS.
E2.148	System and Information Integrity	The EPS must provide on priority basis, and as soon as possible, alerts (e.g. using correlation rules) following indications of compromise or potential compromise and notify Canada.
E2.149	System and Information Integrity	The EPS must prevent all non-privileged users from circumventing intrusion detection and prevention capabilities.
E2.150	System and Information Integrity	The Contractor must implement a centrally managed Integrity Verification Solution to detect unauthorized changes to software and EPS component configuration including: a) performing integrity scans at least every 30 days, and b) automatically generating a Security Incident Ticket upon discovering discrepancies during integrity verification.
E2.151	Data Security & Information Lifecycle Management Data Inventory / Flows	The EPS policies and procedures must be established to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's applications and network and systems. In particular, Contractor must ensure that data that is subject to geographic residency requirements not be migrated beyond its defined bounds.

EPS RFP ID	Requirement Category	Description
E2.152	Data Security & Information Lifecycle Management Non-Production Data	The EPS production data must not be replicated or used in non-production environments.
E2.153	Encryption & Key Management Entitlement	The EPS PKI keys must have identifiable owners (binding keys to identities) and there must be key management policies.
E2.154	Encryption & Key Management Key Generation	The EPS operational policies and procedures must be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, Contractor must inform the GC of changes within the cryptosystem, especially if the EPS data is used as part of the service, or the customer (tenant) has some shared responsibility over implementation of the control.
E2.155	Encryption & Key Management Sensitive Data Protection	The EPS operational policies and procedures must be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.
E2.156	Encryption & Key Management Storage and Access	The EPS platform and data-appropriate encryption (in compliance with CSE guidance ITSG-111 https://www.cse-cst.gc.ca/en/node/1428/html/25015) in open/validated formats and standard algorithms must be required. Keys must not be stored in the cloud (i.e. at the EPS Cloud Contractor in question), but administered by the GC or trusted key management Contractor as mutually agreed upon with Canada. The EPS key management and key usage must be separated duties.
E2.157	Governance and Risk Management Data Focus Risk Assessments	The EPS risk assessments associated with data governance requirements must be conducted at planned intervals as mutually agreed upon with Canada and must consider the following: a) Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network; b) Compliance with defined retention periods and end-of-life disposal requirements; and c) Data classification and protection from unauthorized use, access, loss, destruction, and falsification.

EPS RFP ID	Requirement Category	Description
E2.158	Governance and Risk Management Management Oversight	The EPS managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.
E2.159	Governance and Risk Management Management Program	The Contractor must have an Information Security Management Program (ISMP) developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program must include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: a) Risk management b) Security policy c) Organization of information security d) Asset management e) Human resources security f) Physical and environmental security g) Communications and operations management h) Access control i) Information systems acquisition, development, and maintenance
E2.160	Governance and Risk Management Risk Management Framework	All EPS risks must be mitigated to an acceptable level. Acceptance levels based on risk criteria must be established and documented.
E2.161	Zone Internetwork Device Partitioning	The EPS use of virtual devices in the zone internetwork must be sufficiently partitioned from virtual servers in all zones for containing applications of EPS.
E2.162	Storage Partitioning	EPS Storage used by the hypervisor for virtual device images must be physically and/or logically partitioned for EPS containing applications of PROTECTED B with MEDIUM injury as defined by Canada.
E2.163	Use of Hypervisor Features	The EPS Design Specific Virtual machines must not use any machine to machine sharing mechanism (e.g. file sharing) which is implemented within the hypervisor
E2.164	Hypervisor Certification	The Contractor must use current or previously evaluated hypervisors managing all zones, as defined within the CSE ITSG-22 (https://cse-cst.gc.ca/en/node/268/html/15236) & ITSG-38 (https://cse-cst.gc.ca/en/node/266/html/25034) guidelines, (https://cse-cst.gc.ca/en/canadian-common-criteria-scheme/main) validated under a recognized Common Criteria scheme against an approved Protection Profile that considers hypervisor evaluation for virtual machines protection between zones or obtain approval from Canada for alternative products.

EPS RFP ID	Requirement Category	Description
E2.165	& Virtualization Security Management - Vulnerability Management	The Contractor must ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g. virtualization aware) within the EPS.
E2.166	& Virtualization Security Production / Non-Production Environments	The EPS production and non-production environments must be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties as approved by Canada.
E2.167	& Virtualization Security Segmentation	The Contractor's multi-tenant EPS-owned or managed (physical and virtual) applications, and system and network components, must be designed, developed, deployed and configured such that provider and GC (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: a) Established policies and procedures; b) Isolation of business critical assets and/or sensitive user data, and sessions that mandate stronger internal controls and high levels of assurance; and c) Compliance with legal, statutory and regulatory compliance obligations.
E2.168	Interoperability & Portability Virtualization	The Contractor must use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and must have documented custom changes made to any hypervisor in use and all EPS-specific virtualization hooks available for GC review.
E2.169	Privacy Impact Assessment	As requested by the crown, the Contractor must actively participate in the conduct of a privacy impact assessment on the EPS in accordance with the TBS Privacy Impact Assessment Policy (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510).
E2.170	Physical and Environmental Protection	The Contractor must a) screen individuals prior to authorizing access to the information system in accordance with the *TBS Personnel Screening Standard*; b) Rescreen individuals according to conditions requiring rescreening; and c) For Foreign Contractors, see Part 6, 6.1(a) of Security and Privacy Requirements for Foreign Suppliers (personnel Screening).
E2.171	Physical and Environmental Protection	The Contractor must a) satisfy the personnel security control requirements including security roles and responsibilities for third-party providers. b) document personnel security control requirements. c) monitor provider compliance. d) ensure security screening of private sector organizations and individuals who have access to Protected information and assets.

EPS RFP ID	Requirement Category	Description
		e) explicitly define government oversight and end-user roles and responsibilities relative to third-party provided services.
E2.172	Physical and Environmental Protection	a) The Contractor is responsible for recruitment of personnel. b) The Contractor must: • maintain an updated list which clearly identifies personnel by name, title, responsibility, completed training, and facility and systems access levels as set out in the SOW • submit the list to the Project Authority when requested. • keep an employee record file which can demonstrate that the personnel have the necessary qualifications to perform the work. Such employee record file must be submitted to the Project Authority upon request • Throughout the term of the contract provide the Project Authority with an updated criminal record check and credit check report for all or any personnel upon request, at the Contracting Authority's discretion. • keep the security screening documentation on file and available to the Contracting Authority for each employee for a period of ten (10) years following the initial offer of employment. • rescreens individuals according to conditions requiring rescreening.
E2.173	Operational Security	The Contractor must a) ensure that all activities carried out in relation to the Security and Privacy requirements in the Statement of Work (SOW), provides comparable levels of protection to those identified in GC policies as well as meets or exceeds industry standard or best practice (e.g. ISO 27001), whichever is greater. b) upon request by the Contracting Authority, provide proof of compliance with legislation in the country of operation which may include, but is not limited to, compliance with national laws concerning privacy protection, adherence to tax laws, incorporation regulations, labour laws. c) identify an authorized Company Security Officer (CSO) to be responsible for overseeing the privacy and security requirements of Personal Information processed as a result of the Contract. This individual will be the point of contact for privacy and security matters, in collaboration with the Contracting Authority as well as to work with the Contracting Authority for Access to Information (ATIP) requests. The CSO will be accountable for monitoring the application of privacy and security practices and responding to audit comments. Further information on the appointment of and responsibilities of a CSO can be found at: http://ssi-iss.tpsgc-pwgsc.gc.ca/msi-ism/ch1/intro-eng.html#ch1-103 . d) assign a principal IT security contact with a functional reporting relationship to security management who will ensure that the following functions are performed: i. Establish and manage the Contractor's IT security program as part of the overall security approach; ii. Identify, define and document information system security roles and responsibilities;

EPS RFP ID	Requirement Category	Description
		iii. Make recommendations regarding approval of all contracts for external providers of IT security services; iv. Work with program and service delivery managers to ensure their IT security needs are met, provide advice on safeguards and advise of potential impacts of new and existing threats and on the residual risk of a program or service; v. Monitor departmental compliance with security standards; and vi. Establish an effective process to manage IT security incidents, and monitor compliance

SECTION II – SAMPLE SECURITY REQUIREMENTS TRACEABILITY MATRIX

Table 2 below provides a sample Security Requirements Traceability Matrix (SRTM).

						Security Assessment & Authorization (SA&A) Gates		
EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.1	Access Control	The Contractor must a) develop, disseminate, and review/update annually, the access control policies and associated access control requirements for EPS components; and b) provide GC with the operational security procedures that include operational roles and responsibilities for access control.						
E2.2	Access Control	The Identity Credential and Access Management Service must automatically provision Accounts for EPS User Accounts and Generic Accounts, as follows: a) assign a unique EPS Account and Display Name in accordance with the standard defined in SOW, by applying configurable naming and conflict resolution rules; b) create an Account with no privileges; c) assign a one-time temporary password to the Account; d) assign Account attributes and security access privileges as specified by GC; and e) return the assigned EPS Account, Display Name, and one-time password to the Account Requester.						