Annex A SOW - Appendix B, IIS Security Controls

This Appendix contains security control requirements for the Internet Interconnection Services (IIS) selected from the Information Technology Security Guidance - IT Security Risk Management: A Lifecycle Approach - Security Control Catalogue - ITSG-33 – Annex 3 (http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/itsg33-ann3-eng.html). The Contractor must refer to ITSG-33 – Annex 3 for a complete description of the Controls and the Control Enhancements.

Notes:

a) DSol refers to Draft Solicitation, provided during RFRE process.
b) SOW refers to the Statement of Work attached to the RFRE.
c) References to clauses found in the solicitation and SOW are in addition to the tailored ITSG-33 Protected A, Medium Assurance, Medium Availability (PALL) profile.
d) Not all security clauses from the solicitation and SOW are included in this profile. Clauses that appear in the Solicitation or SOW have references to the heading and paragraph.
e) The Security Requirements Traceability Matrix (SRTM) must demonstrate compliance with security related clauses in the solicitation and SOW, as well as requirements stated in this control profile.
f) EIET refers to Electronic Information Exchange Tool.

SRTM #	Family	Control ID	Enhancement	Name	IIS Clauses and additional ITSG-33 Controls for Security Assessment & Authorization (SA&A)
SRTM 1	AC	2		ACCOUNT MANAGEMENT	The Contractor must manage IIS Solution Service Infrastructure 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 SSC IIS Solution Service Infrastructure 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 SSC IIS Solution Service Infrastructure Operators are terminated, transferred, or SSC IIS Solution Service Infrastructure 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 SSC, and iv) temporary and emergency accounts over a given age; l) granting access to the IIS Service Infrastructure based on: i) a valid access authorization; ii) intended system usage, and iii) other attributes as required by the Contractor or SSC; 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.
SRTM 2	AC	2	(2)	ACCOUNT MANAGEMENT	The Contractor must terminate and disable temporary and emergency accounts used in management, incident resolution or troubleshooting of IIS System Components within: (A) 48 hours of remediation of incidents requiring account creation; or (B) one week of inactivity.
SRTM 3	AC	2	(4)	ACCOUNT MANAGEMENT	The EIET, IIS Audit System and, any IIS components deployed at a GC SIP, automatically audit privileged account creation, modification, disabling, and termination actions and notify, as required, appropriate individuals.
SRTM 4	AC	3		ACCESS ENFORCEMENT	The SSC IIS Service Infrastructure must enforce access authorizations for Operators.

SRTM 5	AC	4	INFORMATION FLOW ENFORCEMENT	The Contractor must obtain SSC authorization prior to the implementation and use of information flow control and/or flow modification devices in the IIS service, such as, but not limited to: (A) Firewalls, (B) Application Proxies; (C) Web or content caching devices; (D) Data Loss Prevention; (E) Data and/or Content Compression; (F) Priority of Service; (G) Quality of Service; (H) Social Media Inspection and/or Content Caching; (I) Content substitution (e.g. targeted advertisements); (J) Technology that introduces site redirection [RFRE SOW 2.1 para (36)] The Contractor must ensure that the IP traffic is not shaped in this service. [DSol 7.7.6.4] The Contractor must ensure that all domestic network traffic (meaning traffic initiated in one part of Canada to a destination or individual located in another part of Canada) is routed exclusively through Canada.
SRTM 6	AC	5	SEPARATION OF DUTIES	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.

SRTM 7	AC	6	LEAST PRIVILEGE	The Contractor must implement a least privileges policy for the IIS Infrastructure 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 IIS Solution Service Infrastructure. [DSol 7.7.7.1.1] [The Contractor must] control access to all databases on which any data relating to this Contract is stored so that only individuals with the security clearance required by the Contract, and who also require access to the information in order to perform the Contract, are able to access the database; [DSol 7.7.7.1.2] [The Contractor must] ensure that passwords or other access controls are provided only to individuals who require access to perform the Work and who have the security clearance issued by CISD at the level required by the Contract;
SRTM 8	AC	8	SYSTEM USE NOTIFICATION	IIS infrastructure deployed at a SIP must display an approved system use notification message or banner before granting access to the system that provides privacy and security notices in accordance with the TBS Policy on the Use of Electronic Networks. The notification message or banner must remain on the screen until users take explicit actions to log on to or further access the IIS component.

SRTM 9	AC	17		REMOTE ACCESS	[SOW 5 para (245)] The Contractor must use a secure (encrypted) and trusted connection, which includes strong authentication and auditing of user access along with, non-repudiation of changes and data integrity protection, for remote management and administration of IIS Managed Services, using a process approved by SSC. The Contractor shall make the associated audit logs available to SSC upon request. [DSol 7.7.8.1] The Contractor must ensure that the equipment/all the components that form part of the system used to deliver the network services can be managed using secure protocols. [DSol 7.7.8.2] If the Contractor is using management servers that have a configurable level of security or encryption, the Contractor must disable all levels other than the highest level of security and/or encryption. [DSol 7.7.8.3] The Contractor must not use protocols that send clear text usernames or passwords over the network. [DSol 7.7.8.4] The Contractor must not use (and must disable any) protocols that cannot pass through session aware firewalls. [DSol 7.7.8.5] Canada will not consider an otherwise insecure protocol to be secure as a result of the use of tunnelling techniques such as port forwarding or Internet Protocol Security (IPSec). [DSol 7.7.8.6] The Contractor must implement encryption protocols identified by Canada and must disable all encryption protocols not approved by Canada.
SRTM 10	AC	17	(5)	REMOTE ACCESS	The Contractor must monitor for unauthorized remote connections to IIS components deployed at a GC SIP, and takes appropriate action if an unauthorized connection is discovered.
SRTM 11	AC	22		PUBLICLY ACCESSIBLE CONTENT	The IIS Contractor must obtain SSC approval prior to posting information, including statistics related to, obtained from, or inferred from the contractual engagement with Canada.

SRTM 12	AU	2	AUDITABLE EVENTS	The Contractor must ensure the EIET, IIS Audit System and IIS components deployed at a GC SIP audit the following privileged user/process events at a minimum: (a) Successful and unsuccessful attempts to access, modify, or delete security objects (Security objects include audit data, system configuration files and file or users' formal access permissions.) (b) Successful and unsuccessful logon attempts (c) Privileged activities or other system level access (d) Starting and ending time for user access to the system (e) All program initiations In addition, the information system audits the following unprivileged user/process events at a minimum: (a) Successful and unsuccessful attempts to access, modify, or delete security objects (b) Successful and unsuccessful logon attempts (c) Starting and ending time for user access to the system

SRTM 13	AU	3	CONTENT OF AUDIT RECORDS	The IIS Contractor must ensure IIS System Components produce 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. [DSol 7.7.7.3] The Contractor must maintain an audit log that automatically records all attempts to access Canada's network, as well as any databases that include Canada's data or information maintained by the Contractor about Canada (such as billing information and call detail information). Every action, transaction or business function performed on the Contractors network, systems, or databases relating to the Contract must be traceable to an individual user or account (by ensuring that user identifiers and accounts are unique and cannot be shared or transferred from one individual to another).
SRTM 14	AU	4	AUDIT STORAGE CAPACITY	The IIS Contractor must not drop audit events as a result of availability of storage capacity.

SRTM 15	AU	5	RESPONSE TO AUDIT PROCESSING FAILURES	The Contractor must ensure any audit processing failures in the EIET, IIS Audit system, or IIS components deployed at a GC SIP alert designated Contractor organizational officials and are included in reports provided by the EIET.

SRTM 16	AU	6	AUDIT REVIEW, ANALYSIS, AND REPORTING	The IIS Contractor must review and analyze IIS SIP component security audit records weekly for indications of inappropriate or unusual activity, and report findings to SSC IT Security Coordination Centre (ITSCC) officials. The Contractor must adjust the level of audit review, analysis, and reporting when there is a change in risk to the IIS Contractor's operations, assets, individuals, other organizations, or Canada, based on law enforcement information, intelligence information, or other credible sources of information.

SRTM 17	AU	6	(1)	AUDIT REVIEW, ANALYSIS, AND REPORTING	The Contractor must adjust the level of audit review, analysis, and reporting within the information system when there is a change in risk to the IIS Contractor's operations, assets, individuals, other organizations, or Canada, based on law enforcement information, intelligence information, or other credible sources of information.

SRTM 18	AU	8	TIME STAMPS	The IIS Contractor must ensure IIS System Components synchronize internal system clocks with an authoritative time source, approved by SSC to generate time stamps for audit records.

SRTM 19	AU	9	(4)	PROTECTION OF AUDIT INFORMATION	The Contractor must restrict access to management of IIS audit functionality to only a limited subset of privileged users.
SRTM 20	AU	11		AUDIT RECORD RETENTION	[SOW 8.9 para (383)] The Contractor must retain the security violations, transactions, audit records, and alarm incident records and associated reports for the current and previous 2 years, and must obtain SSC's written permission to destroy any records after 2 years.

SRTM 21	CA	2	SECURITY ASSESSMENTS	[SOW 3.6.6 Para (157) The Contractor must provide a Security Architecture Report to SSC that describes for the Contractor's infrastructure: c) How Security Assessment and Authorization is addressed in accordance to ITSG-33 in support of continuous monitoring and mitigation while assessing the performance of common security controls of the information support systems.

SRTM 22	CA	5	(1)	SAFEGUARDS IMPLEMENTATION PLAN (PLAN OF ACTION AND MILESTONES)	[SOW 3.6.5 para (156)] The Contractor must provide a Security Risk Management Plan to SSC that includes: a) How security risks will be reported (to whom and at what frequency); b) Roles and responsibilities toward security risk management; and c) How security risks will be tracked and addressed.
SRTM 23	CM	2		BASELINE CONFIGURATION	[SOW para 5.2 (270)] Configuration Management performed by the Contractor for the IIS must include: a) The configuration and programming of all features and functions and modifications of hardware and software components to meet the on-going operational requirements of the IIS in accordance with Canada's requirements; b) Implementing hardware and software fixes; c) Maintaining configuration information and status on all hardware and software

					components; d) Backing up configuration files, incremental changes on a daily basis, and maintaining the backup configuration files off-site; e) Maintaining configuration log files that will include an entry for each configuration change where each entry in the configuration log file must include: i) Date and time of configuration change; and ii) Resource making the configuration change; f) Providing the configuration information of hardware and software components when requested by Canada within 5 FGWDs of a request, in a file naming convention as specified by Canada and Commercial Off-the-Shelf (COTS) file format that is approved by Canada; g) Maintaining the current and previous copies of configuration information; and h) Tracking the status of a configuration item as it changes from one state to another (e.g. for instance 'under development', 'being tested', 'live', or 'withdrawn').
SRTM 24	CM	2	(5)	BASELINE CONFIGURATION	The IIS Contractor must develop, maintain, restrict and control the list of applications, software programs and processes authorized to execute on the EIET.

SRTM 25	CM	6	CONFIGURATION SETTINGS	[SOW 8.1 para (354)] The Contractor must protect the EIET and its information according to industry standards and best practice such as using intrusion detection systems, antivirus software, firewalls and IP filtering routers. (353.d) The Contractor must lock down access to the EIET by IP addresses and application port numbers. [DSol 7.7.7.3] Unless requested by the Technical Authority, the Contractor must disable any TCP/UDP listening ports on any equipment deployed on Canada's network or on the Contractors network infrastructure or backbone with which Canada's network is interconnected. Strong access control methods must be in place for all ports that are open for network management purposes.
SRTM 26	CM	7	LEAST FUNCTIONALITY	The Contractor must apply and implement a least-privilege principle for IIS system components and the EIET.
SRTM 27	CM	8	INFORMATION SYSTEM COMPONENT INVENTORY	[SOW 7.2 para (338)] The Contractor is required upon special request to provide to Canada a special inventory report on equipment implemented at SSC's sites for the IIS, within 10 FGWDs of a change to the information from the previous report, that includes: a) Equipment owned by the Contractor; b) The manufacturer of the equipment and country of origin; c) The model and serial number of the equipment; d) The date that the equipment was installed; and e) The date on which the Firmware was last updated.

SRTM 28	CM	8	(1)	INFORMATION SYSTEM COMPONENT INVENTORY	The Contractor must update the inventory of information system components deployed at a GC SIP as an integral part of component installations, removals, and information system updates.
SRTM 29	CP	1		CONTINGENCY PLANNING POLICY AND PROCEDURES	[SOW 3.3 para (99)] The Contractor must provide a Service Continuity Plan to SSC for disaster recovery and business resumption of the IIS that includes: a) A strategy for restoring the service; b) Processes that will be used to effect service continuity (for example, communications strategy, service restoration prioritization); c) Transferring operational and management functionality in the primary operations centre to the backup operations centre; d) Back up strategies for facilities, operational support systems and data, and key service components; e) Ensuring that its suppliers (if applicable) have in place disaster recovery plans and strategies; and f) Timeframes that Canada can expect services to be restored.
SRTM 30	CP	2		CONTINGENCY PLAN	[SOW 5.6 para (309)] The Contractor IIS must respond to any failure situation to ensure Internet access availability. [SOW 5.6 para (310)] Availability Management must include: a) Reviewing availability requirements and ensuring contingency plans are put in place and tested on a regular basis to ensure service delivery requirements are met;
SRTM 31	IA	2		IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	The EIET must enforce two-factor authentication using hard crypto token for all privileged Operator accounts in compliance with CSEC ITSG-31 Section 2.2.1.3 Level 3. The Contractor must enforce two-factor authentication for in-band management of IIS components deployed at a GC SIP.

SRTM 32	IA	2	(100)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	IIS system components deployed at a GC SIP require multifactor authentication for remote access to privileged accounts.
SRTM 33	IA	4		IDENTIFIER MANAGEMENT	The IIS Contractor must manage identifiers for users and devices used in management or operation of IIS Infrastructure and Components by; (a) receiving authorization from a designated organizational official to assign a user or device identifier; (b) selecting an identifier that uniquely identifies an individual or device; (c) assigning the user identifier to the intended party or the device identifier to the intended device; (d) preventing reuse of user or device identifiers for 180 days; and (e) disabling the user identifier after 30 minutes of inactivity. The Contractor must not use system account identifiers to manage IIS Infrastructure or components that also match accounts subject to reconnaissance (i.e. harvest of publicly available contact information) methods (e.g. through DNS contact, social media sites, or other technical association with the Contractor)
SRTM 34	IA	5		AUTHENTICATOR MANAGEMENT	The IIS Contractor must manage authenticators for users and devices by: (a) verifying, as part of the initial authenticator distribution, the identity of the individual and/or device 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, for lost/compromised or damaged authenticators, and for revoking authenticators; (e) changing default content of authenticators upon information system installation; (f) establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if applicable); (g) changing and refreshing password-based authenticators no less frequently than 180 days; (h) protecting authenticator content from unauthorized disclosure and modification; and (i) requiring users to take, and having devices implement, specific measures to safeguard

					authenticators.
SRTM 35	IA	5	(1)	AUTHENTICATOR MANAGEMENT	Password-based authentication for the EIET must: [SOW 8.1 para (353.c.1)] Contain at least 6 characters; [SOW 8.1 para (353.c.2)] Change required every 60 days; and [SOW 8.1 para (353.c.3)] Contain upper and lower characters with at least 1 numerical symbol.
SRTM 36	IA	6		AUTHENTICATOR FEEDBACK	The EIET must obscure feedback of authentication information during the authentication process, to protect the information from possible exploitation/use by unauthorized individuals.
SRTM 37	IR	5		INCIDENT MONITORING	[SOW 4.4 para (226)] The Contractor must monitor and report all incidents on a 24/7/365 basis on the services provided to Canada.

SRTM 38	IR	6	INCIDENT REPORTING	[SOW 3.6.8 para (159)] The Contractor must provide notification and generate Security Incident Tickets that include but not limited to the following information: a) Type and description of an attack, b) Whether attack appears to have been successful and impact, c) Attack scope (to one or many client groups), d)Suspected source/origin of attack, incident or event e) actions taken, and f) Status of mitigation. [DSol 7.7.9.1] The Contractor must provide to the Technical Authority timely information about vulnerabilities (i.e., any weakness, or design deficiency, identified in any equipment provided under the Contract/any component that forms part of the system used to deliver the network services that would allow an unauthorized individual to compromise the integrity, confidentiality, access controls, availability, consistency or audit mechanism of the system or the data and applications it hosts.
SRTM 39	MP	1	MEDIA PROTECTION POLICY AND PROCEDURES	The Contractor must, within the Operational Readiness Phase, develop and disseminate media protection and handling policy that addresses the roles, responsibilities, restrictions and compliance with handling of media containing GC logs associated with the provision of the IIS service, including: (A) Physical and logical access to IIS logs and storage media, including temporary, or portable devices used for analysis or transfer of IIS logs; and (B) Destruction processes and procedures for media used to store or process GC logs. (C) Release of media or logs to authorized GC authorities; (D) Data Protection requirements for inclusion of GC logs (Protected A) during communication with GC (excluding EIET).
SRTM 40	MP	2	MEDIA ACCESS	The Contractor must implement access control measures to ensure only authorized individuals may access media containing IIS logs, incident reports, usage patterns and statistics.

SRTM 41	MP	3	MEDIA MARKING	The Contractor must: (a) mark removable information system media and information system output containing or displaying Canada's Protected Information in a manner that clearly indicates the distribution limitations, handling caveats, and applicable security markings (if any) of the information. (b) physically control and securely store digital and non-digital media containing Canada's Protected Information in accordance with the Royal Canadian Mounted Police (RCMP) G1-001, Security Equipment Guide. (c) physically protect and securely store Protected information system media awaiting destruction (either on- or off-site) using SSC approved equipment, techniques, and procedures.
SRTM 42	MP	6	MEDIA SANITIZATION	(a) The Contractor must sanitize information system media containing Canada's Protected Information, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse. (b) The Contractor must employ sanitization mechanisms approved by Canada. (c) The Contractor must track, document, and verify media sanitization and disposal actions.
SRTM 43	PE	2	PHYSICAL ACCESS AUTHORIZATIONS	The Contractor must implement role-based physical access control to its IIS Service Infrastructure facilities where EIET and the Audit system containing IIS logs reside, including: a) keeping an access list of personnel with authorized access to the facilities; b) issuing authorization credentials for access to the facilities; c) reviewing and approving the access list and authorization credentials at all times at least monthly, removing from the access list personnel no longer requiring access; d) authorizing physical access to the facilities, by access point, based on the role of the individual; e) adjust role assignment as Operator role changes to new role; f) implementing separation of duties where the authorization to access facilities is done by a different person than the authorization to access IIS Service Infrastructure; and g) allowing access to facilities to authorized personnel based on a need-to-know and need-to-access. [DSol 7.7.1] The contractor and/or its employees must EACH maintain a valid Reliability Status issued by Public Works and Government Services Canada – Industrial Security Program.

SRTM 44	PE	2	(100)	PHYSICAL ACCESS AUTHORIZATIONS	[DSol 7.7.3.3] Upon arriving at Canada's premises, all Contractor and subcontractor personnel (which have been pre-approved by the Contracting Authority), must be able to provide proof of employment (such as a badge issued by the Contractor or the approved subcontractor) and their security clearance status must be ascertained from a trusted source; The Contractor must issue an identification card to all personnel having a role or responsibility for the IIS service, which as a minimum includes the name of the organization, the bearer's name and photo, a unique card number and an expiry date. The Contractor must require presentation of the identification card as a requirement for physical access authorization to the Contractor's facility where the EIET and IIS Audit System reside.
SRTM 45	PE	3		PHYSICAL ACCESS CONTROL	The IIS Contractor must: (a) Enforce physical access authorizations for all physical access points (including designated entry/exit points) to the facility where IIS Infrastructure and configuration data resides (excluding those areas within the facility officially designated as publicly accessible). (b) Verify individual access authorizations before granting access to the facility. (c) Control entry to the facility containing the information system using physical access devices and/or guards. (d) Control access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk. (e) Secure keys, combinations, and other physical access devices. (f) Maintain an accurate inventory of physical access devices. (g) Change combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated. [RFRE 2.3.1, DSol 7.7.1] The contractor must maintain a valid Document Safeguarding Capability (DSC) at the Protected A level issued by Public Works and Government Services Canada – Industrial Security Program.

SRTM 46	PE	6	MONITORING PHYSICAL ACCESS	The IIS Contractor must: (a) Monitor physical access to the EIET and IIS Audit systems to detect and respond to physical security incidents. (b) Review physical access logs monthly and following suspected incidents. (c) Coordinate results of reviews and investigations with the Contractor's incident response capability.
SRTM 47	PE	16	DELIVERY AND REMOVAL	The IIS Contractor must authorize, monitor, and control storage and handling of IIS Infrastructure components entering and exiting the facility and maintains records of those components, in support of Supply Chain integrity objectives. [DSol 7.7.1] The contractor and/or its employees MUST NOT remove any Protected B, C or CLASSIFIED information or assets from the identified work site(s).
SRTM 48	PL	2	SYSTEM SECURITY PLAN	(A) The IIS Contractor must develop a security plan for the IIS service, EIET and IIS Audit system that: (i) describes the operational environment; (ii) describes relationships with or connections to other IIS Contractors or upstream Providers; (iii) provides an overview of the security control requirements for the IIS service and EIET and IIS Audit system; (iv) describes the security controls in place or planned for meeting those requirements (and the requirements specified in this Control Profile) including a rationale for the tailoring and supplementation decisions; and (v) is reviewed and approved by the SSC Authority prior to plan implementation. (B) The IIS Contractor must review the security plan for the information system annually. (C) The IIS Contractor must update the plan to address changes to the IIS System and environment of operation, or problems identified during plan implementation or security control assessments.

SRTM 49	PL	2	(1)	SYSTEM SECURITY PLAN	[SOW 3.6.4 para (155)] The Contractor must provide a Security Concept of Operations report to Canada that describes the: a) User community; b) Contractor applications used for service operation; c) Contractor data center and communication facilities; d) Security roles and responsibilities of the Contractor; e) Incident Analysis and Post Incident Reporting; f) Access controls; and g) Contractor's operational environment.
SRTM 50	PL	2	(2)	SYSTEM SECURITY PLAN	[SOW 3.6.6 (157)] The Contractor must provide a Security Architecture report to Canada that describes for the Contractor's infrastructure: a) How Public Access Zone (Public Access Zone is described in CSEC publication ITSG-22 [http://www.cse-cst.gc.ca/documents/publications/itsg-csti/itsg22-eng.pdf] and ITSG-38 [http://www.cse-cst.gc.ca/documents/publications/itsg-csti/itsg38-eng.pdf]) interfaces are strictly controlled, including all external controlled networks such as the Internet, at a defined security perimeter; b) How other network security zones are established in accordance with the Communication Security Establishment Canada ITSG-22; c) How Security Assessment and Authorization is addressed in accordance to ITSG-33 in support of continuous monitoring and mitigation while assessing the performance of common security controls of the information support systems. d) The equipment used by the Contractor in the provisioning of IIS directly and indirectly interfacing with Government of Canada infrastructure (e.g. Routers) must have previously received validation under a recognized Common Criteria scheme, either against an approved Protection Profile, of if one does not exist, an applicable security target, whose assurance requirements conform either to EAL 2 or an approved assurance package. e) Cryptographic modules employed in accessing the EIET, shall be validated to the FIPS 140-2 standard or subsequent standards, to encrypt communications between the Government of Canada and the Contractor. f) The FIPS 140-2 validated cryptographic modules shall be configured to operate in FIPS mode, in order to utilize only CSEC approved algorithms and key sizes. CSEC approved algorithms and key sizes are documented in IT Security Alert 11 Version E, (ITSA-11E) and are subject to change. g) The Contractor must include a brief overview description of the network diagrams provided.

SRTM 51	PS	3		PERSONNEL SCREENING	[SOW 8.4 para (370.a.13)] ... the Contractor must obtain personnel security (SECRET) clearances and Canadian Citizenship for their employees, individuals and any subcontractor personnel, involved in providing the service to GC, including conducting the management, administration and support of those components.
SRTM 52	PS	4		PERSONNEL TERMINATION	(a) The Contractor, upon termination of individual employment must terminate the individual's logical and physical access to the IIS Infrastructure and components. (b) The Contractor, upon termination of individual employment must retrieve all IIS security-related information and property from the individual.
SRTM 53	SA	3		LIFE CYCLE SUPPORT	(A) The Contractor must manages the EIET and IIS Audit systems using a system development life cycle methodology that includes information security considerations. (B) The Contractor must define and document roles and responsibilities throughout the system development life cycle. (C)The Contractor must identify individuals having information system security roles and responsibilities.
SRTM 54	SA	4	(7)	ACQUISITIONS	SOW 3.6.6 Para (157) d) The equipment used by the Contractor in the provisioning of IIS directly and indirectly interfacing with Government of Canada infrastructure (e.g. Routers) must have previously received validation under a recognized Common Criteria scheme, either against an approved Protection Profile, of if one does not exist, an applicable security target, whose assurance requirements conform either to EAL 2 or an approved assurance package.

SRTM 55	SA	5		INFORMATION SYSTEM DOCUMENTATION	(A)The Contractor must obtain, protect as required, and make available to authorized personnel and Canada upon request, administrator documentation for the EIET, IIS Audit System, and IIS components at a GC SIP, that describes: (i)Secure configuration, installation, and operation of the information system; (ii)Effective use and maintenance of security features/functions; and (iii)Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions. (B)The organization obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes: (i)User-accessible security features/functions and how to effectively use those security features/functions; (ii)Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and (iii)User responsibilities in maintaining the security of the information and information system. (C)The organization documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.
SRTM 56	SA	12	(2)	SUPPLY CHAIN PROTECTION	[DSol 7.8.1] At any time during the Contract, if the Contractor proposes introducing new commercial products, that were not on the IT Products List approved by Canada, on Canada's network or on the Contractor's own or 3rd party infrastructure or backbone that will be interconnected with Canada's network, the Contractor must first obtain the written approval of the Technical Authority. Canada reserves the right to refuse new commercial products, propose new safeguards and to independently validate and approve the commercial products. [DSol 7.8.2] At any time, if Canada notifies the Contractor that any given manufacturer or OEM is no longer considered a trusted manufacturer or OEM (i.e. un-trusted), the Contractor (and its subcontractors) must immediately cease deploying equipment made by that manufacturer or OEM in Canada's network and in any infrastructure or backbone of the Contractor that will interconnect with Canada's network. For already deployed equipment, the Contractor has to identify and/or remove equipment made by that manufacturer or OEM in Canada's network and in any infrastructure or backbone of the Contractor that will interconnect with Canada's network. If Canada requests a change as per this section the Contractor shall be entitled to an equitable adjustment. [DSol 7.8.3] If the Contractor becomes aware that any third party (other than a

				subcontractor) is deploying untrusted equipment on its network, the Contractor must immediately notify the Technical Authority.
SRTM 57	SC	2	APPLICATION PARTITIONING	The IIS Contractor must use physical or logical measures to ensure separation of user functionality (including user interface services) from management functionality for the EIET, IIS Audit System and any IIS component deployed at a GC SIP. [DSol 7.7.6.2] The Contractor must ensure that all databases on which any data relating to this Contract is stored/archived are physically and logically independent (meaning there is no direct or indirect connection of any kind) from all other databases.
SRTM 58	SC	5	DENIAL OF SERVICE PROTECTION	[SOW 2.6 para (72)] The Contractor must provide the ability to analyze the IP traffic to and from the Internet, and detect and remove (i.e. scrub) malicious IP traffic based upon signatures, reputation and IP traffic anomalies. The Contractor must provide the capability for SSC to obtain and export meta data and logs associated with a real or suspected cyber attack. [SOW 2.6 para (85)] The Contractor must provide Anti-DDOS systems with initial protection capacity of 2Gbps of Internet Bandwidth, with the option to increase this capacity upon request in 1Gbps steps. [SOW 2.6 para (86)] The Contractor must be able to mitigate up to five (5) ongoing attack streams, including black hole mitigations, with the option to increase this number, based on demand.
SRTM 59	SC	7	BOUNDARY PROTECTION	The Contractor must implement security zoning of the EIET and IIS Audit System, in accordance with guidelines set forth in the CSEC ITSG-22 **[Section 3 Network Security Zones and IT Security]** guidance document. [DSol 7.7.6.3] The Contractor must ensure that all data relating to this Contract is accessed and processed only in Canada or in an alternate jurisdiction approved by the Contracting Authority under paragraph

SRTM 60	SC	7	(11)	BOUNDARY PROTECTION	[SOW 8.1 para (353.d)]The Contractor must lock down access to the EIET by IP addresses and application port numbers.
SRTM 61	SC	10		NETWORK DISCONNECT	The Contractor must ensure EIET sessions and boundary systems protecting the EIET, terminate sessions when initiated by an end-user or after 30 minutes of inactivity.
SRTM 62	SC	12		CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	[DSol 7.7.3.1] The Contractor acknowledges that Canada may specify some equipment or networks as security sensitive and select a security classification in which case only security cleared employees and contractors may work on the system. Non-cleared persons may only assist in working on the system but not actually control or load software. The Contractor's SOC must use a Secure Terminal Equipment (STE), provided as Government Furnished Equipment, following existing COMSEC processes, to communicate with Canada when requested by Canada that includes a unique and dedicated telephone number. The Contractor must designate a COMSEC custodian as an interface for the purposes of facilitating cryptographic key management of the STE and performing basic testing and troubleshooting as requested by Canada.
SRTM 63	SC	13		USE OF CRYPTOGRAPHY	[SOW 3.6.6 (157)] (e) Cryptographic modules employed in accessing the EIET, shall be validated to the FIPS 140-2 standard or subsequent standards, to encrypt communications between the Government of Canada and the Contractor. (f) The FIPS 140-2 validated cryptographic modules shall be configured to operate in FIPS mode, in order to utilize only CSEC approved algorithms and key sizes. CSEC approved algorithms and key sizes are documented in IT Security Alert 11 Version E, (ITSA-11E) and are subject to change. [SOW 8.1 para (353.e)] The Contractor must implement Transport Layer Security (TLS) on

					the EIET, [if a web-based solution is implemented,] and must encrypt the web session using 3 Key Triple Data Encryption Algorithm (3DES) or Advanced Encryption Standard (AES).
SRTM 64	SC	23	(1)	SESSION AUTHENTICITY	The Contractor must ensure the EIET invalidates session identifiers upon user logout or other session termination.
SRTM 65	SC	23	(2)	SESSION AUTHENTICITY	The EIET must provide a readily observable logout capability.
SRTM 66	SI	2		FLAW REMEDIATION	The Contractor must identify and correct EIET and IIS Audit System flaws. The Contractor must incorporate flaw remediation into the Contractor's configuration management process.

SRTM 67	SI	3	MALICIOUS CODE PROTECTION	The Contractor must ensure the EIET and IIS Audit systems are protected from direct or indirect consequences of malicious code.
SRTM 68	SI	4	INFORMATION SYSTEM MONITORING	(a) The Contractor must monitor events on the EIET, IIS Audit system, and IIS Infrastructure to detect: i. information system attacks, ii. conditions that may adversely affect availability or integrity of the IIS service. iii. Evidence of breach of confidentiality to Canada's Protected Data, including but not limited to the contents of data stored in the EIET, IIS Audit System, or any communication system used in the communication of Protected Data or Protected Voice conversations. (b) The Contractor must identify and report unauthorized use of the IIS System and Infrastructure, EIETl and IIS Audit System to the SSC Technical Authority. (c) The Contractor must deploy Government Furnished Equipment (GFE) monitoring devices: (i) strategically within the Contractor's Facilities and Infrastructure to collect essential information related to the service provided to Canada; and (ii) at ad-hoc locations within the information system to track specific types of transactions of interest to the Contractor. (d) The Contractor must provide a means for the transportation of all Government of Canada GFE monitored IP layer traffic to a location within the National Capital Region to be specified by Canada. (e) The Contractor must heighten the level of IIS System and Infrastructure monitoring activity whenever there is an indication of increased risk to the Contractor's operations and assets, individuals, other organizations, or Canada, based on law enforcement information, intelligence information, or other credible sources of information. (f) The Contractor must obtain legal opinion with regard to information system monitoring activities in accordance with Government of Canada legislation and Treasury Board Secretariat policies, directives and standards. [SOW 2.6 para (84)] The Contractor must be proactive through continual monitoring for cyber threats from Denial of Service attacks and provide notifications followed up by mitigation recommendations to SSC when and if the Contractor is made aware of cyber

					threats targeting SSC, that may potentially impact the Government of Canada Network and implement the mitigations, once approved by SSC.
SRTM 69	SI	4	(5)	INFORMATION SYSTEM MONITORING	[SOW 2.6 para (71)] When ordered, the Contractor must provide Anti-Distributed Denial of Service (Anti-DDOS) Scrubbing Service within the Contractor's infrastructure. [SOW 2.6 para (77)] The Contractor must send near-real time alerts to Canada either through email or text message based on configured key trigger or intrusion events. Trigger or intrusion events include, but are not limited to: (a) Denial of Service control channels to/from Canada's IIS Service deployment points. (b) Denial of Service or Distributed Denial of Service attacks against GC address space.
SRTM 70	SI	5		SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	(a) The Contractor must receive and action information system security alerts, advisories, and directives from organizations as designated by Canada on an ongoing basis. (b) The Contractor must generate internal security alerts, advisories, and directives as deemed necessary. (c) The Contractor must disseminate security alerts, advisories, and directives to all personnel involved in the administration, operation, investigation or incident handling of the IIS System, IIS Service, and IIS Infrastructure. (d) The Contractor must implement Canada provided security directives related to elevated threats or persistent threats in accordance with established time frames. [DSol 7.7.2.2] The Contractor acknowledges that Canada requires, and the Contractor guarantees that, the telecommunications services provided under the Contract is and will be the subject of robust, comprehensive security measures that evolve as security threats and technologies evolve, so that the security measures in use are updated throughout the Contract Period, in order to achieve the highest possible levels of data integrity, availability, and confidentiality. [DSol 7.7.2.3] The Contractor must implement any reasonable security or protection measures requested by Canada from time to time, within a reasonable timeframe agreed to with Canada. The parties agree that reasonableness will be determined based on the severity of the threat to the integrity, availability and confidentiality of Canada's data and

				communications. [SOW 2.6 para (91)] The Contractor must react to the demands of SSC in the case where SSC advises the Contractor of an eminent cyber threat.
SRTM 71	SI	12	INFORMATION OUTPUT HANDLING AND RETENTION	The Contractor must handle and retain information within and output from the IIS Service in accordance with applicable GC legislation and TBS policies, directives and standards, and operational requirements.
SRTM 72	CA	7	CONTINUOUS MONITORING	[DSol 7.7.10.1] The Contractor must monitor the network for abnormal or suspicious activities, such as odd work hours, unnecessary requests for code or data, abnormal data movements, or excessive use of systems or resources. [DSol 7.7.10.2] The Contractor must immediately report to the Technical Authority and CISD any incidents relating to the security of Canada's network, or the Contractors network infrastructure or backbone, or Canada's data, if it impacts Canada, including but not limited to those incidents listed in ([DSol] 7.6.12.1). For example, any unauthorized access or attempt to gain unauthorized access must immediately be reported. Also, the discovery of any virus or malicious code and/or the installation of any unauthorized software code on any equipment must immediately be reported.