IIS RFRE 10026415/A			
Questions and Answers 3			
Question	**Section**	**Industry Question**	**SSC Response**
22EN	Annex A: SOW (Draft RFP)	In Annex A Statement of Work, Introduction item (3), Canada states that: "SSC has currently designed the Government of Canada Network (GC.Net) with special routing arrangements that permit the re-routing of its Internet Protocol (IP) traffic when one or more SIPsfail." Please confirm that the contractor(s) responsible for the Inbound load sharing.	SSC will manage the load sharing and the failover between Contractors' SIPs.
22FR	Annexe A: Énoncé des travaux (Version provisoire de la demande de propositions (DP)	Le point 3 de l'Introduction de l'annexe A, Énoncé des travaux, se lit comme suit : « Services partagés Canada (SPC) a configuré le réseau du Canada avec des arrangements de routage spéciaux qui permettent le réacheminement de son trafic avec protocole Internet (IP) lorsqu'un ou plusieurs des PIS [points d'interface de service] subissent une panne de service. » Veuillez confirmer que la répartition de chargement des données entrantes relève de la responsabilité des entrepreneurs.	SPC gérera la répartition de chargement et le basculement entre les points d'interface de service (PIS) des entrepreneurs.

IIS RFRE 10026415/A			
Questions and Answers 3			
Question	**Section**	**Industry Question**	**SSC Response**
25EN	Annex D – Draft Bid Solicitation	Section 2.3.1 requests that “The contractor and/or its employees must EACH maintain a valid Reliability Status issued by Public Works and Government Services Canada – Industrial Security Program. Section 7.7.3.4 indicates “These individuals are to be security screened and granted a Security Clearance to a minimum of SECRET. Examples include technical or operational personnel, including network or system administrators or managers, who directly control the most sensitive and critical functionality such as monitoring, detection, backup and recovery information, testing and installation of security patches, configuration changes to security hardware and software, responding to security incidents etc.” Annex A: SOW (Draft RFP), Section 8.4.4 Security Management Procedures, indicates Personnel Security Clearances, whereby 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. Please confirm that Section 2.3.1 will be updated to reflect SECRET .	The SRCL and associated Clauses in RFRE Annex D - DRAFT RFP, Part 7 will be changed to reflect SECRET in the Final RFP.

IIS RFRE 10026415/A			
Questions and Answers 3			
Question	**Section**	**Industry Question**	**SSC Response**
25FR	Annexe D: Version provisoire de la demande de propositions (DP)	Selon le point 2.3.1, l'entrepreneur ou son personnel « doivent TOUS maintenir une cote de fiabilité valide délivrée par le Programme de sécurité industrielle de Travaux publics et Services gouvernementaux Canada. » Selon le point 7.7.3.4, « Ces personnes doivent faire l'objet d'une enquête de sécurité et obtenir une habilitation de sécurité du niveau SECRET au moins. Par exemple, le personnel technique ou opérationnel, y compris les administrateurs ou les gestionnaires de réseaux ou de systèmes, qui contrôle directement les fonctionnalités les plus sensibles et essentielles comme la surveillance, la détection, la sauvegarde et la récupération de l'information, la mise à l'essai et l'installation de correctifs de sécurité, les changements de configuration au matériel et au logiciel de sécurité, la réaction aux incidents de sécurité, etc. » Le point 8.4.4, Procédures de gestion de la sécurité, de l'annexe A de l'Énoncé des travaux (EDT) [DP provisoire], indique les attestations de sécurité du personnel, selon lesquelles chacun des employés de l'entrepreneur, et toute personne ou employé d'un sous-traitant de l'entrepreneur, qui contribuera à la prestation du service pour le Canada, y compris la gestion, l'administration et le soutien technique de ces composants, doit détenir une attestation de sécurité du personnel cotée SECRET et la nationalité canadienne..	La Liste de vérification des exigences relatives à la sécurité (LVERS) et les clauses connexes dans l'annexe D de la demande de réponses pour l'évaluation (DRPE) – Partie 7 de la demande de propositions provisoire seront modifiées pour que la demande de propositions définitive indique le niveau SECRET.
26EN	Annex A: SOW (Draft RFP)	Please provide an attachment with all required security controls (e.g. ITSG 33 controls).	See attached File: Annex D Draft RFP, Annex A SOW, Appendix B IIS Security Controls. The SOW will be updated in the Final RFP to state, "the security profile is still subject to change and this will be clarified during the Operational Readiness Phase following contract award."
26FR	Annexe A : Énoncé des travaux	Veuillez fournir une pièce jointe comprenant tous les contrôles de sécurité requis (comme les Conseils en matière de sécurité – ITSG-33).	Voir le fichier ci-joint : annexe D – Demande de propositions provisoire, annexe A – Énoncé des travaux, appendice B – Contrôles de sécurité du SII. Dans la demande de propositions définitive, l'EDT sera corrigé comme suit : « le profil de sécurité peut toujours faire l'objet de changements, ce qui sera clarifié à l'étape de la préparation opérationnelle à la suite de l'attribution du marché ».

IIS RFRE 10026415/A			
Questions and Answers 3			
Question	**Section**	**Industry Question**	**SSC Response**
43EN	Annex D – Draft Bid Solicitation, 7.7.3 Security Clearance, 7.7.3.4	Section 7.7.3.4 states that Individuals, although not having access to CLASSIFIED information or assets, may occupy positions that are deemed to be critical to the national interest. This includes personnel who have privileged access that give them the capability to effect major disruption or damage to critical systems. These individuals are to be security screened and granted a Security Clearance to a minimum of SECRET. However, SRCL Section 7C states that the level of information is Protected A and Part B of the SRCL states the Security level screening required is Protected A, therefore Reliability Clearance is required. As clearances are predicated on the level of sensitivity of information that might or will be accessed, the SRCL requirement is not consistent with the requirement for a SECRET clearance. Can Canada clarify the security clearance requirements to address this ambiguity in the current wording?	The SRCL and associated Clauses in RFRE Annex D - DRAFT RFP, Part 7 will be changed to reflect SECRET in the final RFP.
43FR	Annexe D: Version provisoire de la demande de propositions (DP) Article 7.7.3.4	Selon le point 7.7.3.4, « Des personnes qui, même si elles n'ont pas accès à l'information ou des biens CLASSIFIÉS, peuvent occuper des postes qui sont jugés essentiels à l'intérêt national. » Il s'agit entre autres du personnel qui a un accès privilégié offrant la possibilité de perturber ou d'endommager de façon importante des systèmes essentiels. Ces personnes doivent faire l'objet d'une enquête de sécurité et obtenir une habilitation de sécurité du niveau SECRET au moins. Toutefois, le point 7C de la LVERS indique que le niveau d'information est Protégé A, et la partie B de la LVERS indique que le niveau de filtrage de sécurité requis est Protégé A, par conséquent une cote de fiabilité est nécessaire. Comme les cotes se fondent sur le degré de confidentialité de l'information à laquelle les personnes auront ou pourront avoir accès, l'exigence contenue dans la LVERS ne correspond pas à l'exigence d'une cote de niveau SECRET. Le Canada peut-il préciser les exigences relatives à la cote de sécurité en clarifiant l'ambiguïté soulevée par les termes utilisés?	La Liste de vérification des exigences relatives à la sécurité (LVERS) et les clauses connexes dans l'annexe D de la demande de réponses pour l'évaluation (DRPE) – Partie 7 de la demande de propositions provisoire, seront modifiées pour que la demande de propositions définitive indique le niveau SECRET.

IIS RFRE 10026415/A			
Questions and Answers 3			
Question	**Section**	**Industry Question**	**SSC Response**
44EN	RFRE Annex B: Security Requirements Checklist (SRCL)	Section 6 (b) of the SRCL states that maintenance personnel will not have access to restricted areas. (a) Can Canada clarify if this is intended to also refer to vendor access to the Canada service delivery points? (b) If so, how would personnel required for installation and maintenance of equipment on the Canada sites be able to support the SOW requirements without having access?	The SRCL and associated Clauses in RFRE Annex D - DRAFT RFP, Part 7 will be changed to reflect SECRET in the final RFP.
44FR	DPRE Annexe B: Liste de vérification des exigences relatives à la sécurité	Selon le point 6 (b) de la LVERS, le personnel d'entretien n'aura pas accès aux zones d'accès limité. (a) Le Canada peut-il préciser si cette restriction s'applique aussi à l'accès des fournisseurs aux points de prestation de service du Canada? (b) Dans l'affirmative, comment le personnel responsable de l'installation et de l'entretien du matériel dans les installations du Canada pourra-t-il se conformer aux exigences de l'EDT sans avoir accès aux installations?	La Liste de vérification des exigences relatives à la sécurité (LVERS) et les clauses connexes dans l'annexe D de la demande de réponses pour l'évaluation (DRPE) – Partie 7 de la demande de propositions provisoire seront modifiées pour que la demande de propositions définitive indique le niveau SECRET.
46EN	Annex A - Draft SOW, Sections 4.3 Contractor's IIS Service Desk & 4.4 Service Operation and Monitoring para (209) and (223)	It is not industry standard to provide customers direct access to Contractor's internal ticketing systems. Contractors usually provide customers with a 1-800 number or an email ID for communication on troubles. Will Canada accept a view of the Incident tickets via the EIET?	This change is agreed to and will be reflected in the Final RFP. SSC will accept a view of the incident tickets via the EIET as along as a near-real time view (no more than 15 minutes delay) is provided.
46FR	Annexe A: Section 4.3 et 4.4, paragraphs (209) et (223)	Il n'est pas la norme dans l'industrie de donner aux clients accès aux systèmes de gestion internes de l'entrepreneur. Les entrepreneurs fournissent habituellement aux clients un numéro de téléphone 1-800 ou une adresse courriel pour communiquer les problèmes. Le Canada acceptera-t-il de donner accès aux dossiers d'incident au moyen de l'outil électronique d'échange d'information?	Ce changement est acceptable et sera réflété dans la version finale de la demande de proposition. SPC acceptera de voir les dossiers d'incidence par le biais de l'outil électronique d'échange d'information seulement si un aperçu en temps quasi réel (un délai ne dépasant pas 15 minutes) est fourni.

IIS RFRE 10026415/A			
Questions and Answers 3			
Question	**Section**	**Industry Question**	**SSC Response**
60EN	Annex C IT Products List	The information the Crown is requesting (esp. hardware & software details and release information) is considered to be HIGHLY CONFIDENTIAL to Suppliers and releasing it without having a signed NDA between parties is considered a SERIOUS security risk. As part of the RFRE process, and in advance of submission, will SSC sign an NDA with suppliers in order to obtain this information?"	Under SACC Manual Clause 2003, the Crown has obligated itself to treat the information as confidential pursuant to (5)6.
60FR	Annexe C : Liste des produits de technologie de l'information (TI)	Les renseignements demandés par l'État (notamment les détails sur le matériel et les logiciels, et l'information sur les versions) sont considérés par les fournisseurs comme TRÈS CONFIDENTIELS, et leur diffusion sans qu'une entente de confidentialité soit signée entre les parties représente un risque SÉRIEUX en matière de sécurité. Dans le cadre du processus de la DRPE et avant la présentation d'une réponse, SPC signera-t-il une entente de confidentialité avec les fournisseurs dans le but d'obtenir de tels renseignements?	Selon le sous-alinéa 6 de l'article 05 de la clause 2003 du Guide des CCUA, l'État a l'obligation de traiter ces renseignements comme confidentiels.
61EN	Annex A, Section: 2.5 Additional Bandwidth Required under Special Situations	Has the government taken into consideration the interconnectivity (peering) issues between ISP's as well as their selected ISP access to the greater public Internet? Such interconnectivity issues often arise outside of the selected vendor's ISP network as not all end users who may need to gain access to services inside the government's data center originate their request from within the government's selected ISP; specifically in Canada, ISP's in the Western Provinces do not peer with one another and thus traffic requests originating in Vancouver and requiring termination in Ottawa are routed first through an IXP in Seattle, across the Rocky Mountains and finally up through the Peering Point in either OTTIX or TORIX. This leads to very slow access for those requesting end users. Has the government considered asking for additional services from the ISP, such as a distributed computing platform independent of their own ISP, which can mitigate congestion, ISP failure, and latency on both the selected ISP as well as the Internet as a whole?	SSC has identified an acceptable performance metrics such as the Throughput and transit delay.

IIS RFRE 10026415/A			
Questions and Answers 3			
Question	**Section**	**Industry Question**	**SSC Response**
61FR	Annexe A, Section 2.5 Bande passante supplémentaire requise dans des situations particulières	Le gouvernement a-t-il tenu compte des problèmes d'interconnectivité (apparaige) entre les fournisseurs d'accès Internet (FAI) ainsi que l'accès des FAI sélectionnés à Internet grand public? Des problèmes d'interconnectivité se produisent souvent à l'extérieur du réseau du FAI retenu parce que tous les utilisateurs finals qui demandent l'accès aux services dans le centre de données du gouvernement le font par l'intermédiaire du FAI sélectionné du gouvernement. Au Canada, cette situation concerne particulièrement les provinces de l'Ouest où il n'y a pas d'interconnexion entre les FAI. Ainsi, les demandes de trafic provenant de Vancouver à destination d'Ottawa sont d'abord acheminées par un point d'échange Internet (IXP) à Seattle, au-dessus des Rocheuses, puis par l'intermédiaire d'un point d'appairage dans OttIX (Ottawa Internet eXchange) ou TorIX (Toronto Internet eXchange). Le résultat est un accès très lent pour les utilisateurs finals à l'origine des demandes. Le gouvernement a-t-il envisagé de demander des services supplémentaires au fournisseur d'accès Internet (FAI), comme une plateforme répartie indépendante du FAI, ce qui pourrait diminuer la congestion, les pannes et la latence pour les deux FAI sélectionnés et	SPC a établi des mesures de rendement acceptables comme le débit de données et le délai de transit.
62EN	2.6 Anti-Distributed Denial of Service Scrubbing Service	The government has asked for "(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." The requirement as written is streamlined to focus only on IP traffic. Has the government considered also leveraging a service that is application aware (such as web based HTTP, HTTPs services, and DNS services), as opposed to focusing only on IP packet scrubbing? Given that these attack vectors are becoming very prevalent in today's threat environment, the government might find it very beneficial to include such a service capability request.	SSC is requesting Internet Services with integrated Anti-DDoS protection. The proposal in this question appears to be focused more on a specific Anti-DDoS service from an overall managed security services perspectives which is out of scope for this procurement.

IIS RFRE 10026415/A			
Questions and Answers 3			
Question	**Section**	**Industry Question**	**SSC Response**
62FR	2.6 Service de nettoyage anti-déni de service distribué	Le gouvernement a demandé que l'entrepreneur offre « (72) la possibilité d'analyser le trafic IP provenant d'Internet ou acheminé vers le réseau Internet, et de détecter et de supprimer (nettoyer) le trafic IP malveillant selon les signatures, la réputation et les anomalies du trafic IP » et qu'il permette « à SPC d'obtenir et d'exporter des métadonnées et des journaux associés à une cyber-attaque réelle ou présumée. » Tel qu'elle est rédigée, cette exigence porte uniquement sur le trafic IP. Le gouvernement a-t-il aussi envisagé de mettre à profit un service compatible avec les applications (comme HTTP Web, les services HTTP et les services DNS [serveur de noms de domaine]) au lieu de se concentrer sur le nettoyage des paquets de données IP? Comme ces vecteurs d'attaque sont très courants dans l'environnement actuel où abondent les menaces, le gouvernement tirerait de gros avantages à demander de tels services.	SPC demande des services Internet avec une protection anti-déni de service distribué intégrée. Dans cette question, la proposition semble surtout porter sur un service anti-déni de service distribué particulier conformément au point de vue général de la gestion des services de sécurité, ce qui ne fait pas partie de la portée de ce marché.
63EN	2.6 Anti-Distributed Denial of Service Scrubbing Service	Has the government considered, as opposed to limiting responses to discrete centralized scrubbing centers located on a single ISP, using a highly distributed multi-ISP deployed, multi-country mitigation service distributed across at least 1,000 different ISP's in order to stop attacks in proximity to the attack's origin?	Refer to the answer to question 62
63FR	2.6 Service de nettoyage anti-déni de service distribué	Le gouvernement a-t-il envisagé d'utiliser un service d'atténuation à répartition élevée, déployé dans de nombreux pays et FAI, réparti dans au moins 1 000 FAI différents, afin d'arrêter les attaques à proximité de leur point d'origine, au lieu de limiter les réponses à de simples centres de nettoyage centralisés situés chez un seul FAI?	Veuillez consulter la réponse à la question 62.
64EN	2.6 Anti-Distributed Denial of Service Scrubbing Service	Has the government considered leveraging a security service designed to mitigate web based attacks from within the attacker's ISP (or logically close to it), as opposed to waiting for the attacker's traffic to be routed to the government's subscribed to ISP (or scrubbing center) for mitigation?	Refer to the answer to question 62
64FR	2.6 Service de nettoyage anti-déni de service distribué	Le gouvernement a-t-il envisagé d'utiliser un service de sécurité conçu pour réduire les attaques Web à partir du FAI du pirate informatique (ou logiquement à proximité) au lieu d'attendre que les données du pirate soient acheminées au FAI (ou centre de nettoyage) du gouvernement aux fins d'atténuation?	Veuillez consulter la réponse à la question 62.
65EN	2.6 Anti-Distributed Denial of Service Scrubbing Service	Has the government considered web traffic DDoS mitigation service that remains "on" 100% of the time AND without causing any performance degradation, and can begin mitigating attacks immediately, without delay?	Refer to the answer to question 62

IIS RFRE 10026415/A			
Questions and Answers 3			
Question	**Section**	**Industry Question**	**SSC Response**
65FR	2.6 Service de nettoyage anti-déni de service distribué	Le gouvernement a-t-il envisagé d'avoir un service Web d'atténuation des attaques de déni de service distribué qui est disponible en tout temps, n'entraîne aucune perte de rendement ET peut commencer à atténuer les attaques immédiatement, sans délai?	Veuillez consulter la réponse à la question 62.
66EN	2.6 Anti-Distributed Denial of Service Scrubbing Service	Has the government considered a service that can also implement an "inline" Web Application Firewall (WAF) in additional to layer 3 / layer 4 DDoS volumetric defense?	Refer to the answer to question 62
66FR	2.6 Service de nettoyage anti-déni de service distribué	Le gouvernement a-t-il envisagé un service qui permet de mettre en œuvre un pare-feu d'applications Web « en ligne » en plus d'une protection volumétrique contre les attaques de déni de service distribué dans les couches 3 et 4?	Veuillez consulter la réponse à la question 62.
67EN	2.6 Anti-Distributed Denial of Service Scrubbing Service	Has the government considered leveraging a service capable of terminating TLS/SSL traffic and applying security policy based on the content of that traffic as well as mitigating target resource exhaustion due to high volumes of TLS/SSL connections required by HTTPs based attacks (as are common in the Global Financial Services Industry)?	Refer to the answer to question 62
67FR	2.6 Service de nettoyage anti-déni de service distribué	Le gouvernement a-t-il envisagé d'utiliser un service capable de mettre fin au trafic de données utilisant les protocoles TLS ou SSL et d'appliquer une politique de sécurité fondée sur le contenu du trafic, et aussi d'atténuer la surutilisation des ressources visées en raison de volumes élevés de connexions TLS ou SSL requises par les attaques liées au code HTTP (courantes dans l'industrie mondiale des services financiers)?	Veuillez consulter la réponse à la question 62.
68EN	2.6 Anti-Distributed Denial of Service Scrubbing Service	Has the government considered using a service designed to mitigate not only high volume DDoS attacks but also low volume web based attacks (e.g. SlowLoris, RUDY, SlowPOST,etc.) designed to tie up origin processing resources with low volumes of traffic?	Refer to the answer to question 62
68FR	2.6 Service de nettoyage anti-déni de service distribué	Le gouvernement a-t-il envisagé d'utiliser un service conçu pour atténuer non seulement le volume élevé d'attaques de déni de service distribué, mais aussi les attaques Web de faible volume (p. ex. SlowLoris, RUDY, SlowPOST) conçues pour immobiliser les ressources de traitement d'origine par un trafic réduit ou de faibles volumes?	Veuillez consulter la réponse à la question 62.
69EN	2.6 Anti-Distributed Denial of Service Scrubbing Service	Has the government considered a DDoS mitigation service that can successfully discriminate attacker versus non-attacker web based traffic? Such a service need to be able to handle effectively and intelligently traffic which emanates from behind a large proxy or NAT'ed service provider and can thus reduce false positives.	Refer to the answer to question 62

IIS RFRE 10026415/A			
Questions and Answers 3			
Question	**Section**	**Industry Question**	**SSC Response**
69FR	2.6 Service de nettoyage anti-déni de service distribué	Le gouvernement a-t-il envisagé d'utiliser un service d'atténuation des attaques de déni de service distribué qui peut différencier le trafic Web piraté de celui qui ne l'est pas? Un tel service doit pouvoir traiter efficacement et intelligemment un trafic qui provient d'un important fournisseur de service de procuration ou de traduction d'adresses réseau, pouvant ainsi réduire le nombre de faux positifs.	Veuillez consulter la réponse à la question 62.
70EN	2.6 Anti-Distributed Denial of Service Scrubbing Service	The government has asked for "(85) The Contractor must provide Anti-DDOS systems with initial protection capacity of 2 Gbps of Internet Bandwidth, with the option to increase this capacity upon request in 1Gbps steps".	SSC is requesting that the Anti-DDoS service ensure that 2Gbps of Internet bandwidth remains available – regardless of the size of attack.
70FR	2.6 Service de nettoyage anti-déni de service distribué	Le gouvernement a demandé que (85) l'entrepreneur puisse fournir des systèmes de déni de service distribué offrant une capacité de protection initiale de deux Gbps sur la bande passante Internet, avec la possibilité d'augmenter cette capacité sur demande de un Gbps à la fois.	SPC demande que le service anti-déni de service distribué garantisse que deux Gbps de la bande passante Internet demeurent disponibles – peu importe l'importance de l'attaque.
71EN	2.6 Anti-Distributed Denial of Service Scrubbing Service	As of the first quarter of 2013, the average DDoS attack has been measured by the Industry in the 30+ Gbps range. Is the government aware that they are asking for initial protection well below the new average threshold of attacks? Might the government, instead require a DDoS solution that can mitigate today's average web based DDoS attacks between 30 and 50 Gbps and can immediately, and dynamically, scale to hundreds of Gbps without the need to deploy any new hardware or change customer defense configurations?	SSC is requesting that the Anti-DDoS service ensure that 2Gbps of Internet bandwidth remains available – regardless of the size of attack.
71FR	2.6 Service de nettoyage anti-déni de service distribué	Pour le premier trimestre de 2013, les attaques de déni de service distribué mesurées par l'industrie étaient en moyenne supérieures à 30 Gbps. Le gouvernement est-il conscient qu'il demande une protection initiale bien inférieure à la nouvelle limite moyenne des attaques? Le gouvernement ne devrait-il pas plutôt envisager d'acquérir une solution anti-déni de service distribué qui peut atténuer les attaques de déni de service distribué sur le Web, dont la moyenne actuelle se situe entre 30 et 50 Gbps, et passer immédiatement et de manière dynamique à des centaines de Gbps sans qu'il soit nécessaire de déployer du nouveau matériel ou de changer les configurations de protection des clients?	SPC demande que le service anti-déni de service distribué garantisse que deux Gbps de la bande passante Internet demeurent disponibles – peu importe l'importance de l'attaque.
72EN	Section 4.3 (208)	Would the government be willing to remove the requirement of accepting emails and acknowledgements, as well as increasing the notification period to 30 minutes?	Canada will not change this requirement.
72FR	Section 4.3 (208)	Le gouvernement serait-il disposé à supprimer l'exigence relative à l'acceptation des courriels et les avis de réception et à fixer la période de notification à 30 minutes?	Le Canada ne modifiera pas cette exigence.
75EN	Section 4.4 (231)	Would the government be willing to remove the requirement to have read access to the ticketing system?	Refer to answer 46.

IIS RFRE 10026415/A			
Questions and Answers 3			
Question	**Section**	**Industry Question**	**SSC Response**
75FR	Section 4.4 (231)	Le gouvernement serait-il disposé à supprimer cette exigence pour avoir accès en lecture au système de gestion des appels de dépannage?	Voir la réponse 46.
76EN	Section 4.5 (236 - 238)	This may infringe the privacy rights of other customers if access to all databases is provided. Can this requirement be modified? Under 237, can the government provide us with a specific example of why you would need access to our databases?	As mentioned in paragraph (237), GC is only interested in accessing data related to the IIS contract which is GC specific. No requirement for accessing other ISP clients' information.
76FR	Section 4.5 (236 - 238)	Si l'accès à toutes les bases de données est autorisé, une telle exigence peut empiéter sur les droits à la protection de la vie privée des autres clients. Cette exigence peut-elle être modifiée? Concernant le paragraphe 237, le gouvernement peut-il nous fournir un exemple précis qui explique pourquoi il doit avoir accès à nos bases de données?	Comme il est mentionné dans ce paragraphe (237), le gouvernement du Canada souhaite seulement avoir accès aux données liées au marché du SII, qui concerne le gouvernement seulement. Il n'y a pas d'exigence relativement à l'accès aux renseignements des autres clients des FAI.
82EN	Annex D – Draft Bid Solicitation Section 7.7.6.2	Section 7.7.6.2 states 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. A bidder's network performance data is gathered and aggregated from the core network. In order for bidders to provide physically independent databases for any stored/archived data for the Internet and DDOS service will require a customized build for Canada. This successful bidder will need to build a customized standalone solution for 1 circuit, potentially 2 if they are the winner of the NCR and TOR. The costs to build physically separated databases for data related to billing, incidents, reports, etc. is cost prohibitive and will significantly increase costs to Canada. In order to provide the most competitive price to Canada the service should allow for commercial services to be used. We recommend that section 7.7.6.2 be re-worded as follows: The Contractor must ensure that all databases on which any solution data relating to this Contract is stored/archived are logically and securely separated.	Refer to the answer for question 12

IIS RFRE 10026415/A			
Questions and Answers 3			
Question	**Section**	**Industry Question**	**SSC Response**
82FR	Annexe D: Version provisoire de la demande de propositions (DP) Section 7.7.6.2	Selon le point 7.7.6.2, « L'entrepreneur doit s'assurer que toutes les bases de données comprenant des données relatives au présent et archivées sont isolées sur les plans physique et logique, en d'autres termes qu'elles n'ont aucune connexion directe ou indirecte de quelque type que ce soit avec d'autres bases de données. » Les données sur le rendement du réseau du soumissionnaire sont recueillies et regroupées à partir du réseau principal. Pour que les soumissionnaires puissent fournir des bases de données isolées sur le plan physique et comprenant les données stockées ou archivées du service Internet et du service anti-déni de service distribué, il faudra fournir au Canada une solution personnalisée. Le soumissionnaire retenu devra créer une solution autonome personnalisée pour un circuit ou peut-être deux, si ces services sont retenus à la fois pour la région de la capitale nationale et la région de Toronto. Les coûts de création de bases de données physiquement distinctes comprenant les données de facturation, d'incidents, des rapports, etc. sont prohibitifs et augmenteront considérablement les coûts du Canada. Pour offrir au Canada le prix le plus concurrentiel possible, il faudrait permettre l'utilisation des services commerciaux. Nous recommandons que le point 7.7.6.2 soit reformulé comme suit : l'entrepreneur doit s'assurer que toutes les bases de données	Voir la réponse à la question 12
84EN	Attachment 4.1 Mandatory Technical Evaluation	Please confirm that one project reference that covers M001, M002, and M003 is acceptable.	SSC will accept one project reference providing it demonstrates that the bidders meet the requirement.
84FR	Pièce jointe 4.1 : Critères obligatoires de l'évaluation technique	Veuillez confirmer que la référence à un seul projet pour les critères obligatoires O-001, O-002 et O-003 est acceptable.	SPC acceptera un projet de référence qui montre que le soumissionnaire satisfait à l'exigence.
85EN	Annex A: SOW (Draft RFP) (186)	Canada requires Contractor to provide a Service Manager that will act as Canada's initial point of contact for IIS service issues. There is no requirement for a Business Manager function in the SOW, despite SOW 307 & SOW 308 requiring Contract Review meetings. We recommends that Canada add a requirement for a Business Manager that will act as Canada's point of contact for day to day business management including SOW items including 307, 308, 311	A requirement will be added in the Final RFP to read "The Contractor must identify and provide resource(s) who will act as Canada's initial point of contact for IIS service and/or day to day business management issues".

IIS RFRE 10026415/A			
Questions and Answers 3			
Question	**Section**	**Industry Question**	**SSC Response**
85FR	Annexe A : Énoncé des travaux (186)	Le Canada exige que l'entrepreneur ait un gestionnaire de service qui agira à titre de personne-ressource initiale concernant les problèmes de service associés au SII. Il n'y a pas d'exigence relativement à un gestionnaire de service dans l'énoncé des travaux, même si les paragraphes 307 et 308 de l'EDT traitent de l'exigence de réunions d'examen du contrat. Nous recommandons que le Canada ajoute une exigence relative à un gestionnaire de service qui agira comme personne-ressource auprès du Canada pour les questions de gestion courante, y compris les activités décrites dans l'EDT, notamment aux paragraphes 307, 308 et 311.	Une exigence sera ajoutée dans la demande de propositions définitive et se lira comme suit : « L'entrepreneur doit désigner et fournir une ou des ressources qui agiront comme personnes-ressources initiales auprès du Canada concernant le service du SII ou les problèmes de gestion opérationnelle courants. »
86EN	Annex A: SOW (Draft RFP) (246)	As per SOW 246, Contractors can implement Change Requests, excluding Emergency Changes, during maintenance windows as approved by SSC. Please revise the Availability formula in Item 391 to include Scheduled Outage Time: (Expected Service Availability for the month – SSC Approved Scheduled Outage time) - Cumulative Outage for the Month X 100% _____ (Expected Service Availability for the month –Scheduled Outage time)	The formula will remain unchanged as expected Availability by definition includes the deduction for scheduled maintenance and outages that have been approved by SSC in advance as specified in SoW Line 400 b) Scheduled maintenance interruptions approved by SSC.
86FR	Annexe A : Énoncé des travaux (246)	Selon le paragraphe 246 de l'EDT, l'entrepreneur doit exécuter les demandes de changement non urgentes durant les périodes de maintenance approuvées par SPC. Veuillez réviser la formule de la disponibilité indiquée au paragraphe 391 pour y ajouter le temps d'interruption prévu, comme suit : (Disponibilité du service attendue pour le mois – temps d'interruption approuvé par SPC) – temps d'interruption durant le mois X 100 % _____ (disponibilité du service attendue pour le mois – temps d'interruption prévu)	La formule demeurera inchangée puisque la disponibilité prévue comprend par définition la déduction du temps d'interruption pour l'entretien qui a été approuvé au préalable par SPC, comme il est indiqué à la ligne 400 b) de l'EDT : « des interruptions de maintenance prévues et approuvées par SPC ».

IIS RFRE 10026415/A			
Questions and Answers 3			
Question	**Section**	**Industry Question**	**SSC Response**
88EN	Annex A: SOW (Draft RFP) Section 4.3, Contractor's IIS Service Desk (200)	Please confirm SSC will be the only point of contact to the contractors IIS service desks, and calls from SSC partners will go to SSC. End-Users will contact their departmental Service Desk.	SSC will be the only point of contact to the Contractor's IIS service Desk where a specific list of individuals and/or email addresses approved by SSC will be authorized to communicate with the Contractor's IIS Service Desk.
88FR	Annexe A : Énoncé des travaux Section 4.3, Bureau de service du SII de l'entrepreneur (200)	Veuillez confirmer que SPC sera le seul point de contact pour le bureau de service du SII de l'entrepreneur et que les appels des partenaires de SPC seront adressés à SPC. Les utilisateurs finals communiqueront avec le bureau de service de leur ministère.	SPC sera le seul point de contact du bureau de service du SII de l'entrepreneur, et seules les personnes figurant sur la liste de personnes ou d'adresses courriel approuvée par SPC seront autorisées à communiquer avec le bureau de service du SII de l'entrepreneur.
91EN	Annex A: SOW (Draft RFP) Section 2.4 Support for IPv4 and IPv6 Multi-Cast	We recommend removing this requirement, as multi-cast Internet is not industry best practice. Inclusion will drive development cost to providers, increasing pricing to Canada	This requirement will remain unchanged.
91FR	Annexe A : Énoncé des travaux Section 2.4 Soutien pour la diffusion groupée d'IPv4 et d'IPv6	Nous recommandons de supprimer cette exigence puisque la diffusion groupée par Internet ne fait pas partie des meilleures pratiques de l'industrie. L'inclusion de cette exigence entraînera des coûts de développement pour les fournisseurs, ce qui augmentera les prix payés par le Canada.	Cette exigence demeure telle quelle.
92EN	Annex A: SOW (Draft RFP) Section 8.2 IP Traffic Data (353)	We recommend removing this requirement, as real-time reporting of IP traffic data is not industry standard. Inclusion will drive development cost to providers, increasing pricing to Canada.	This requirement will be removed in the Final RFP, another requirement for SNMP read access to the Contractor IIS router will be added in section 4.4 of the SOW so SSC can have a real-time view of the IP traffic.
92FR	Annexe A : Énoncé des travaux Section 8.2 Données sur le trafic IP (353)	Nous recommandons de supprimer cette exigence puisque la production de rapport en temps réel sur les données du trafic IP ne fait pas partie des pratiques de l'industrie. L'inclusion de cette exigence entraînera des coûts de développement pour les fournisseurs, ce qui augmentera les prix payés par le Canada.	Cette exigence sera supprimée dans la demande de propositions définitive. Une autre exigence concernant l'accès en lecture du protocole de gestion de réseau simple (SNMP) du routeur du SII de l'entrepreneur sera ajoutée au point 4.4 de l'EDT, afin que SPC obtienne une vue en temps réel du trafic IP.
93EN	Annex A: SOW (Draft RFP) Section 8.2 IP Traffic Data- (354)	We recommend this requirement be modified as below to avoid development costs and minimize pricing to Canada: *The Contractor must store 15-minute aggregate IP for IPv4 and IPv6 traffic data for the last 14 days and this data must be available for query on the EIET.*	This requirement will remain unchanged.

IIS RFRE 10026415/A			
Questions and Answers 3			
Question	**Section**	**Industry Question**	**SSC Response**
93FR	Annexe A : Énoncé des travaux Section 8.2 Données sur le trafic IP (354)	Nous recommandons que cette exigence soit modifiée comme ci-dessous pour éviter les coûts de développement et réduire les coûts du Canada : *L'entrepreneur doit conserver les données cumulatives sur le trafic IP ainsi que sur les trafics IPv4 et IPv6 distincts enregistrées aux 15 minutes au cours des 14 derniers jours et les rendre accessibles sur le portail Web aux fins d'interrogation.*	Cette exigence demeure telle quelle.
94EN	Annex A: SOW (Draft RFP) Section 8.2 IP Traffic Data- (355),	We recommend this requirement be modified as below to avoid development costs and minimize pricing to Canada: *The Contractor must store 30-minute aggregate IP for IPv4 and IPv6 traffic data for the last 14 days and this data must be available for query on the EIET.*	This requirement will remain unchanged.
94FR	Annexe A : Énoncé des travaux Section 8.2 Données sur le trafic IP (355)	Nous recommandons que cette exigence soit modifiée comme suit pour éviter les coûts de développement et réduire les coûts du Canada : *L'entrepreneur doit conserver les données cumulatives sur le trafic IP ainsi que sur les trafics IPv4 et IPv6 distincts enregistrées aux 30 minutes au cours des 14 derniers jours et les rendre accessibles sur le portail Web aux fins d'interrogation.*	Cette exigence demeure telle quelle.
95EN	Annex A: SOW (Draft RFP) Section 8.2 IP Traffic Data- (356)	We recommend this requirement be modified as below to avoid development costs and minimize pricing to Canada: *The Contractor must store 2-hour aggregate IP for IPv4 and IPv6 traffic data for the last 14 days and this data must be available for query on the EIET.*	This requirement will remain unchanged.
95FR	Annexe A : Énoncé des travaux Section 8.2 Données sur le trafic IP (356)	Nous recommandons que cette exigence soit modifiée comme suit pour éviter les coûts de développement et réduire les coûts du Canada : *L'entrepreneur doit conserver les données cumulatives sur le trafic IP ainsi que sur les trafics IPv4 et IPv6 distincts enregistrées aux 2 heures au cours des 14 derniers jours et les rendre accessibles sur le portail Web aux fins d'interrogation.*	Cette exigence demeure telle quelle.

IIS RFRE 10026415/A			
Questions and Answers 3			
Question	**Section**	**Industry Question**	**SSC Response**
96EN	Annex A: SOW (Draft RFP) Section 8.2 IP Traffic Data- (357),	We recommend this requirement be modified as below to avoid development costs and minimize pricing to Canada: *The Contractor must monitor and record both inbound and outbound IP traffic usage at their respective SIP from the GC.Net every 15 minutes, 24 hours/day, 7 days/week and 365 days/year (24/7/365).*	This requirement will remain unchanged.
96FR	Annexe A : Énoncé des travaux Section 8.2 Données sur le trafic IP (357)	Nous recommandons que cette exigence soit modifiée comme ci-dessous pour éviter les coûts de développement et réduire les coûts du Canada : *L'entrepreneur doit surveiller et enregistrer l'utilisation des données IP entrantes et sortantes à leurs PIS respectifs depuis le réseau GCNet aux 15 minutes, 24 heures sur 24, tous les jours de l'année.*	Cette exigence demeure telle quelle.
97EN	Annex A: SOW (Draft RFP) Section 10	In section 10.1.1 Service Level-Maximum Service Outage Time (SL-MSOT), requirement (394) states: (394) The SL-MSOT for the IIS and for the Anti-DDoS must be less than or equal to 216 minutes (60min.*24Hours*30Days*0.005) or approximately equivalent to 99.5% availability of accumulated outage time 24 hours per day for all days in any 1 (30 day) calendar month. However, in section 10.4 IIS Service Level Table, in the Service Level Requirement column for Availability (SL-IAV), the SL-MSOT requirement states: SL-MSOT: The Contractor's IIS and the Anti-DDoS must be available at all times, with the exception of a maximum of 40 cumulative minutes of outages in any calendar month. Please confirm the "40 cumulative minutes of outage" should be corrected as 216 minutes to be consistent with the (394) SL-MSOT description.	The target availability is 99.5%, however for the purpose of calulating service credits and to encourage faster resolution of outages, the 40 minutes cumulative outage indicated in Table 7 represents the threshold where service credits will start to apply as per Annex D, Part 7, section 7.11.5.1 "Table 1 service credits". This section will be clarified in the Final RFP.

IIS RFRE 10026415/A			
Questions and Answers 3			
Question	**Section**	**Industry Question**	**SSC Response**
97FR	Annexe A : Énoncé des travaux Section 10	Au point 10.1.1 Niveau de service – Temps d'interruption maximal du service (NS-TIMS), l'exigence (394) se lit comme suit : (394) Le NS-TIMS du SII et du service anti-déni de service distribué doit être équivalent ou inférieur à 216 minutes (soit 60 minutes × 24 heures × 30 jours × 0,005) ou environ l'équivalent d'une disponibilité de 99,5 %) de temps d'interruption cumulatif pour une période de 24 heures par jour pour chaque jour d'un mois donné (30 jours). Toutefois, selon le point 10.4, Tableau des niveaux de service du SII, dans la colonne Paramètre du niveau de service – Disponibilité, l'exigence de niveau de service – temps d'interruption maximal du service (NS-TIMS) se lit comme suit : Niveau de service – Temps d'interruption maximal du service (NS-TIMS) : le SII de l'entrepreneur et le service anti-déni de service distribué doivent être offerts en tout temps, à l'exception d'un maximum de 40 minutes cumulatives d'interruption dans un mois civil donné. Veuillez confirmer que les « 40 minutes cumulatives d'interruption » devraient être remplacées par 216 minutes, conformément à la description de NS-TIMS (394).	La disponibilité ciblée est de 99,5 %. Toutefois, pour calculer les crédits de service et encourager la résolution plus rapide des interruptions, les 40 minutes cumulatives d'interruption indiquées au tableau 7 correspondent au seuil à partir duquel les crédits de service commencent à s'appliquer, conformément au « Tableau 1 : Crédits de service » au point 7.11.5.1 dans la partie 7 de l'annexe D. Ce paragraphe sera clarifié dans la demande de propositions définitive.