SERVICES PUBLICS ET APPROVISIONNEMENT CANADA (SPAC)

Modification nº 015 à la demande d'arrangement en matière d'approvisionnement (DAMA) pour

une méthode d'approvisionnement de logiciels-services (SaaS) (Infonuagique GC)

Numéro de référence de la demande de soumissions sur Achatsetventes : EN578-191593/F

LA PRÉSENTE MODIFICATION N^{O} 015 VISE À :	
1.0	Aviser l'industrie de la deuxième série de soumissions qui seront évaluées par le Centre canadien pour la cybersécurité (CCC), et fournir les spécifications sur la façon de présenter une soumission, comme il est indiqué dans la section 1.0, ci-dessous.
2.0	Répondre aux questions reçues concernant la DAMA, comme il est indiqué dans la section 2.0 ci-dessous.
3.0	Partager les questions qui ont été soulevées lors de la journée d'information à l'intention de l'industrie concernant la DAMA logiciels-services le 11 janvier 2021, ainsi que les réponses associées, comme il est indiqué dans la section 3.0 ci-dessous.
4.0	Modifier l'Annexe A — Exigences de qualification, pour modifier les exigences obligatoires 05 et 07 du niveau 1, ainsi que les exigences obligatoires 08 et 011 du niveau 2, comme il est indiqué dans la section 4.0 ci-dessous.
5.0	Remplacer l'Annexe C — Catalogue de solutions de logiciels-services et prix plafonds des services professionnels, dans son intégralité, par une version mise à jour, comme il est indiqué à la section 5.0 ci-dessous.
6.0	Remplacer la partie 6 — Arrangement en matière d'approvisionnement (AMA) dans son intégralité, par une version mise à jour, comme indiqué à la section 6.0 ci-dessous.
7.0	Modifier la partie 7 — Sélection des entrepreneurs et clauses du contrat subséquent, afin de modifier la section 7.2 Sélection de l'entrepreneur et la section 7.3 Processus de demande de soumissions, tel que détaillé dans la section 7.0, ci-dessous.
8.0	Remplacer l'Annexe F — Clauses du contrat subséquent, dans son intégralité, par une version mise à jour, comme détaillé dans la section 8.0, ci-dessous.
9.0	Remplacer l'Annexe H — Exigences relatives à la sécurité pour les fournisseurs étrangers, dans son entièreté, par une version mise à jour, tel que détaillé dans la section 9.0, ci-dessous.
10.0	Fournir à l'industrie une copie de la présentation de la journée de l'industrie sur la DAMA logiciels-services de niveau Protégé.

1.0 Information concernant la deuxième vague de soumissions qui seront évaluées par le CCC durant la deuxième vague d'intégration :

QUESTIONS	RÉPONSES
Q.65 Quand la deuxième série de soumissions sera-t-elle évaluée par le Centre canadien pour la cybersécurité (CCC)?	**R.65** La deuxième vague s'est ouverte à 9 h le 18 janvier 2021 et les soumissions seront acceptées par le Centre de contact de CCC à contact@cyber.gc.ca afin d'intégrer les fournisseurs dans le Programme d'évaluation de la sécurité des TI des logiciels-services du CCC. Le 12 février 2021, à 14 heures, la deuxième période d'intégration sera terminée. Les fournisseurs seront informés de l'heure et de la date de l'ouverture et de fermeture de la troisième période d'intégration via Achatsetventes.
Q.66 Comment faire une soumission pour le programme d'évaluation de la sécurité des TI des logiciels-services du CCC?	**R.66** Conformément à la réponse R.52 publiée dans la modification 011, le processus est le suivant : pour présenter une soumission pour le programme d'évaluation de la sécurité des TI des logiciels-services du CCC, un soumissionnaire doit suivre les étapes suivantes : 1) Demande à obtenir la clé publique nécessaire pour la clé PGP (Pretty Good Privacy) ainsi que le formulaire pour débuter le processus d'intégration en communiquant avec le Centre de contact du CCC, par courriel à l'adresse contact@cyber.gc.ca ou par téléphone en composant le 613-949-7048 ou le 1-833-CYBER-88. L'équipe des services à la clientèle du CCC vous enverra le formulaire et les instructions nécessaires. 2) Vous devrez signer une entente de non-divulgation bilatérale avec le CCC.

QUESTIONS	RÉPONSES
	3) Les fournisseurs qui rencontre les exigences de l'annexe A — Exigences de qualification, pour le niveau 1 (Protégé A) ou niveau 2 (Protégé B) de la DAMA fourniront toute la documentation au Centre canadien de la cybersécurité (CCC). Lors de la fourniture de documents, la clé PGP (Pretty Good Privacy) est recomandé come méthode de chiffrement. Si les fournisseurs utilisent une autre méthode de chiffrement (c'est-à-dire un mot de passe), CCCS peut également collecter des documents à ce moment-là. Pour plus d'informations sur le processus d'intégration, les fournisseurs peuvent se référer à l'Annexe L - Programme d'évaluation de la sécurité informatique (STI) SaaS: Processus d'intégration en vertu de la modification 007 de la DAMA ou / et contacter contact@cyber.gc.ca; et 4) La DAMA se veut un processus de qualification axé sur la collaboration. Si la soumission n'est pas complète, le Centre de contact du CCC communiquera avec le soumissionnaire afin de demander des précisions et/ou les documents manquants.

2.0 Répondre aux questions sur la DAMA

Remarque : Les questions peuvent avoir été modifiées et/ou condensées.

QUESTIONS	RÉPONSES
Q.67 Quel est le niveau de sécurité requis pour obtenir un arrangement en matière 'approvisionnement (AMA) dans le cadre de la présente DAMA?	**R.67** Les fournisseurs doivent détenir les autorisations suivantes pour obtenir un AMA : ADR — Protégé B VOD – Protégé B Le personnel de l'entrepreneur ayant des droits d'accès privilégiés devra également détenir une attestation de sécurité valide de niveau SECRET auprès de la Direction de la sécurité industrielle canadienne. Les fournisseurs étrangers doivent détenir une attestation de sécurité de niveau SECRET et sont encouragés à communiquer avec le responsable de l'arrangement en matière d'approvisionnement afin de demander des renseignements supplémentaires concernant les exigences de sécurité pour les fournisseurs étrangers. Pour plus d'informations sur les exigences de sécurité des contrats internationaux, vous pouvez également visiter: https://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html
Q.68 Dans le cadre du volet 3 : Soumission de revendeurs à valeur ajoutée (RVA), nous comprenons que l'annexe A à soumettre par le RVA doit seulement faire référence aux contrôles de la soumission de l'éditeur de logiciels-services, dans ce cas, le supplément 1 (Schedule 1) de l'Annexe A de l'éditeur de logiciels-services. Est-ce bien cela? En plus du renvoi aux références des réponses de l'éditeur de logiciels-services, y a-t-il des informations/documents spécifiques au RVA qui doivent être soumis dans le cadre de la réponse à l'annexe B?	**R.68** Le Centre canadien de la cybersécurité (CCC), en collaboration avec la Direction de la sécurité industrielle canadienne, exige que les revendeurs titulaires d'AMA aient également besoin des attestations de sécurité de l'industrie décrites dans la DAMA de la Direction de la sécurité industrielle canadienne (DSIC)/ Direction de la sécurité industrielle internationale (DSII) (VOD, ADR et habilitations de sécurité du personnel de niveau approprié).

QUESTIONS	RÉPONSES
Q.69 Dans le cadre du volet 3 : Soumission de revendeurs à valeur ajoutée (RVA), nous comprenons que l'annexe B à soumettre par le RVA doit seulement faire référence aux contrôles de la soumission de l'éditeur de logiciels-services, dans ce cas, l'annexe B1 de l'éditeur de logiciels-services. Est-ce bien cela? En plus du renvoi aux références des réponses de l'éditeur de logiciels-services, y a-t-il des informations/documents spécifiques au RVA qui doivent être soumis dans le cadre de la réponse de l'annexe B?	**R.69** C'est exacte. Rien n'est requis pour répondre à l'annexe B. Il s'agit des obligations courantes en matière de sécurité et de confidentialité.
Q.70 Nous comprenons que les seuls documents spécifiques pour inclure des informations sur les RVA sont le formulaire 1 (signé par le RVA) et le formulaire 3 (signé par l'éditeur de logiciels-services). Est-ce exact?	**R.70** Il faut également fournir le Formulaire 5 — Liste de vérification de l'exhaustivité de la soumission.
Q.71 Le RVA peut-il faire une seule soumission avec plusieurs éditeurs de logiciels-services? Si oui, devrons-nous utiliser le formulaire 1 pour le RVA et le formulaire 3, annexes A, B et D, pour chaque éditeur de logiciels-services?	**R.71** Dans ce scénario, le RVA serait tenu de faire une soumission séparée pour chaque éditeur de logiciels-services.
Q.72 Dans le cas où le RVA voudrait ajouter des éditeurs de logiciels-services supplémentaires à l'avenir, pouvez-vous confirmer que nous avons seulement besoin de fournir le formulaire 3, annexes A, B et D pour chaque éditeur de logiciels-services?	**R.72** Si un RVA souhaite ajouter des éditeurs de logiciels-services supplémentaires, il devra remplir une nouvelle demande pour chaque éditeur de logiciels-services.
Q.73 En ce qui concerne la modification 12, section 4.0 Modification de l'annexe F — Limitation de responsabilité — il semble que la limitation de responsabilité proposée soit différente de la limitation de responsabilité de gestion de l'information/technologie de l'information, et qu'elle élargit la responsabilité du vendeur dans certains domaines. SPAC serait-il disposé à remplacer cette limitation de responsabilité par la limitation de responsabilité de N0000C?	**R.73** La limitation de responsabilité décrite dans la modification 012 a été créée en consultation avec l'industrie et a été approuvée pour être utilisée dans les contrats d'approvisionnement infonuagiques du GC. Le Canada n'est pas disposé à envisager des révisions de la limitation de responsabilité concernant un nuage public.
Q.74 En ce qui concerne le point 6.3, « Clauses et conditions uniformisées », SPAC note que les clauses du guide des CCUA qui en résultent (différentes des conditions générales 2020) sont comme celles qui figurent dans le manuel des CCUA. Est-ce que l'organisme individuel ou SPAC, lorsqu'il émet des demandes de soumissions ou des autorisations de tâches dans le cadre des arrangements en matière d'approvisionnement logiciels-services, citera les conditions générales spécifiques du guide des CCUA (si elles sont différentes de celles de 2020) ou des conditions supplémentaires s'appliqueront-elles à cette demande de soumissions? Sinon, un fournisseur pourrait interpréter cette disposition comme signifiant que toutes les dispositions des CCUA qui « peuvent s'appliquer » à un appel d'offres s'appliqueront, ce qui peut donner un résultat ambigu ou contradictoire.	**R.74** La section 6.3 de la partie 6 de la DAMA fournit le lien vers l'endroit où se trouvent les clauses des CCUA. La section 6.3.1 énonce les clauses et conditions du guide des CCUA qui s'appliquent à la DAMA.
Q.75 Citant le formulaire 3, « Formulaire d'autorisation de l'éditeur de logiciels-services », point ii), les fournisseurs tiers de logiciels-services offrent l'accès à leurs plateformes exclusivement sous réserve de leurs conditions et de leur modèle d'abonnement spécifique. Ils n'accepteront aucune condition nouvelle ou différente qui serait en conflit avec les conditions qu'ils offrent à tout client final, les modifient ou les différencient. La plupart des grands fournisseurs de logiciels-services bien connus exigent que l'utilisateur final accepte et signe un contrat de licence ou d'abonnement directement avec eux pour avoir accès à leur plate-forme et l'utiliser. SPAC reconnaît-il et accepte-t-il de préciser dans cet accord que : a) il	**R.75** Non, SPAC n'accepte pas d'être soumis à des accords de licence d'utilisateur final ou à des conditions générales de tiers. Conformément à la section 3.2(c)(v) de la DAMA, « Seules les modalités de l'ANS relatives aux niveaux de service et à la prestation de service s'appliqueront. Toute modalité de l'ANS non liée aux niveaux de service et à la prestation des services, telles qu'elles sont décrites ci-dessous, sera réputée annulée et ne s'appliquera pas ». La section 3.2(c)(v) précise également que :

QUESTIONS	RÉPONSES
accepte d'être soumis à de telles conditions si la plateforme lui est « revendue » par un fournisseur et b) les conditions de ce fournisseur tiers de logiciels-services prévaudraient sur toute condition incohérente ou contradictoire de la présente DAMA et plus particulièrement sur les conditions relatives à la « solution » de l'annexe F des dispositions du contrat subséquent?	« Les fournisseurs doivent soumettre des accords sur les niveaux de service (ANS) publiés décrivant les accords de niveaux de service à inclure dans l'Annexe D — Accords sur les niveaux de service (ANS). De même, toutes les modalités qui comportent des renseignements sur les prix (comme, mais sans s'y limiter, celles qui tentent d'imposer des conditions financières, des modalités tarifaires ou des pénalités pour non-conformité) figurant à l'annexe D, Accords sur les niveaux de service, seront considérées comme annulées et sont inopérantes. »
Q.76 Concernant l'Annexe F, section 8, « Autorisation de tâches », page 14 : si un fournisseur se voit attribuer un arrangement en matière d'approvisionnement dans le cadre de la présente DAMA, ce fournisseur serait-il obligé de répondre à chaque autorisation de tâches ou à chaque demande de soumissions émise par un ministère autorisé? Autrement dit, un fournisseur peut-il choisir de ne pas répondre à une autorisation de tâches ou à une demande de soumissions dans le cadre de la présente DAMA sans conséquence ni sanction?	**R.76** Les titulaires d'un arrangement en matière d'approvisionnement ne sont pas obligés de répondre à chaque demande de soumissions émise dans le cadre de la DAMA, ni d'accepter tous les contrats ou tâches demandés par un ministère client autorisé dans le cadre d'un arrangement en matière d'approvisionnement. Un fournisseur peut choisir de ne pas répondre à une autorisation de tâches ou à une demande de soumissions dans le cadre de la présente DAMA, et ce, sans conséquence.
Q.77 En règle générale, les services professionnels de logiciels-services exigeraient-ils d'un fournisseur qu'il s'engage également dans des services de cybersécurité pour les environnements de ministères acheteurs, y compris, mais sans s'y limiter, les services de sécurité gérés, les services de cyberdéfense (tels que les tests de pénétration, les services d'évaluation de la vulnérabilité, la recherche des menaces et les services d'intervention en cas d'incidents), ou toute surveillance, analyse, évaluation des tests ou mesures correctives pour les vulnérabilités de sécurité dans les environnements spécifiques du Canada? Si la réponse est oui, le Canada ou ses organismes d'approvisionnement seraient-ils disposés à intégrer dans une autorisation de tâches (AT) des conditions supplémentaires qui établissent des paramètres concernant la nature et les devoirs respectifs associés à ce domaine sensible?	**R.77** Cela ne fait pas partie de la portée des services professionnels inclus dans la DAMA, qui sont limités à ceci : (a) la trousse de formation et de services Guide de démarrage rapide (« GDR ») (b) les services de mise en œuvre; (c) les services de formation; (d) les services d'épuration, de migration et de transition des données; et e) les services consultatifs. Il est également important de noter que chaque AT individuelle émise dans le cadre d'un contrat résultant de l'appel d'offres définira l'étendue des travaux pour cette AT et toute exigence de sécurité qui s'appliquerait aux ressources/entrepreneurs qui exécutent les travaux. Les paramètres des travaux (y compris les exigences de sécurité) seront définis dans les contrats individuels ou les AT émises dans le cadre de l'arrangement en matière d'approvisionnement.
Q.78 Généralités – En raison de la pandémie de COVID-19, le fournisseur a dû adapter son infrastructure pour permettre à son personnel de travailler depuis son domicile jusqu'à ce que les juridictions gouvernementales lèvent les interdictions ou les limitations concernant les modalités de travail en personne et que les conditions de sécurité s'améliorent. À cette fin, le Canada serait-il disposé à inclure une disposition dans l'appel d'offres ou à permettre l'inclusion, dans l'énoncé des travaux ou de l'autorisation de tâches, d'une exigence selon laquelle les parties travailleront ensemble pour faire face aux répercussions sur les services à la lumière de la pandémie de COVID-19 récemment déclarée? Et le fournisseur serait-il en mesure de négocier une autorisation de tâches avec l'organisme d'achat un ensemble de protocoles conçus pour répondre aux exigences qui suivraient ou régiraient le personnel du fournisseur dans la fourniture de services depuis son domicile?	**R.78** Cette question peut être traitée dans les AT individuelles émises dans le cadre des contrats résultant d'un arrangement d'approvisionnement de SaaS. En raison de la pandémie de COVID-19, la plupart des AT que SPAC délivre actuellement précisent que les travaux seront effectués à l'endroit choisi par l'entrepreneur. Toutefois, dans certaines circonstances, cela ne sera pas possible en raison de restrictions de sécurité. Cela peut être discuté avec le service d'achat avant l'émission du contrat ou de l'AT.
Q.79 Lorsque les services de SaaS sont fournis sur la base d'un abonnement (engagements annuels, prépayés), comment cette obligation est-elle conciliée avec la durée du contrat, ou l'absence d'une durée de contrat spécifique? Peut-on s'attendre à ce que les	**R.79** Deux options sont disponibles dans les clauses contractuelles résultantes - l'option utilisée dépendra de la manière dont le SaaS est vendu OU des exigences détaillées dans l'appel d'offres.

QUESTIONS	RÉPONSES
abonnements puissent être résiliés par anticipation ou réduits en volume?	1. La première option est une période contractuelle fixe, où le Canada se retire d'un renouvellement automatique ou ne l'accepte pas, mais souscrit plutôt au SaaS pour une période fixe. 2. La deuxième option est un service d'abonnement sans période contractuelle définie, dans lequel le Canada autorise le renouvellement automatique, mais exige une notification avant le renouvellement automatique, et exige également un délai de grâce de 4 semaines pour résilier le contrat dans le cas où le Canada n'annulerait pas l'abonnement avant le renouvellement automatique. Dans l'une ou l'autre de ces options, le Canada conserve le droit de diminuer la consommation sans pénalité. Les clauses du contrat résultant comprennent également une clause de résiliation pour convenance qui permettrait au Canada de mettre fin aux services et de recevoir un remboursement de tout montant prépayé au-delà du mois où les services sont résiliés.
Q.80 La section 4.1(f) fait référence à « toutes les normes de sécurité requises ». Pourquoi ne fait-elle pas référence aux annexes spécifiques (A et B) qui traitent de la sécurité? Sinon, le libellé est trop vague.	**R.80** La raison pour laquelle il n'est pas fait référence aux annexes spécifiques où les exigences de sécurité sont traitées est qu'il y a de nombreux éléments de sécurité informatique au-delà des annexes A et B, y compris les exigences d'intégrité de la chaîne d'approvisionnement, les exigences de qualification obligatoires (pour les volets 1 et 2), les obligations en matière de sécurité et de protection des renseignements personnels, les exigences de sécurité qui s'appliquent uniquement aux services professionnels et les exigences de sécurité pour l'entrepreneur (comme la VOD, l'ADR et les habilitations du personnel) qui varient selon si l'entrepreneur est canadien ou étranger, ainsi que les exigences qui peuvent s'appliquer au contrat unique d'un client émis dans le cadre de l'AMA de SaaS. Par conséquent, il n'est pas possible de faire référence à toutes les exigences de sécurité qui s'appliqueront à chaque arrangement en matière d'approvisionnement ou à chaque contrat émis dans le cadre d'un arrangement en matière d'approvisionnement à l'étape de la DAMA.
Q.81 La section 5.6 exige une garantie de non-contrefaçon. Que se passe-t-il s'il y a des réclamations relatives à des violations des droits de propriété intellectuelle provenant de chasseurs de brevets qu'un fournisseur est en train de plaider activement. Celles-ci peuvent-elles être exclues de la garantie? Le recours en garantie peut-il être lié exclusivement à l'obligation d'indemnisation?	**R.81** Si un fournisseur a connaissance de réclamations pour violation de la PI, il ne pourra pas certifier « aucune réclamation », mais il pourra néanmoins garantir que, **à sa connaissance**, rien dans la solution, ou dans l'utilisation de la solution par le Canada, **ne viole** ou ne constitue une appropriation illicite de la PI ou d'autres droits d'un tiers. Ces types de réclamations ne peuvent être exclus de la garantie et le recours en garantie ne peut être lié exclusivement à l'obligation d'indemnisation.
Q.82 La section 9.4 (Prix le plus favorable) ne tient pas compte du fait que les obligations supplémentaires que le Canada impose aux vendeurs pour fournir les services de SaaS au Canada et le coût de ces obligations nécessitent probablement une tarification plus élevée que celle appliquée aux autres clients. La section 9.4 devrait être assortie d'une réserve qui inclut des conditions et modalités similaires.	**R.82** Le Canada a examiné cette demande et la formulation de l'attestation de prix détaillée à la section 9.4 reste la même. Bien qu'il puisse y avoir des coûts associés à la qualification pour vendre des solutions de SaaS au gouvernement du Canada, il appartient au fournisseur de déterminer si les avantages de la qualification et de la vente de SaaS au gouvernement du Canada par ce moyen l'emportent sur les coûts. De plus, la clause d'attestation des prix de la section 9.4 fait référence à la qualité et à la quantité des biens, des services ou les deux.
Q.83 L'annexe C comporte un ensemble distinct d'obligations de sécurité. Sont-elles nécessaires en	**R.83** L'annexe C contient des obligations de sécurité permanentes qui s'appliquent pendant toute la durée

QUESTIONS	RÉPONSES
plus des annexes A et B de la DDP? Dans la mesure où il y a un conflit, quelle obligation de sécurité prévaut?	du ou des contrats et qui sont nécessaires pour garantir que le fournisseur continue à remplir ses obligations. Les détails concernant le document qui prévaudra en cas de conflit sont exposés dans la section de la DOC intitulée « Priorité des documents ». L'appendice C relève de l'annexe F - Clauses du contrat résultant, car il s'agit d'un appendice au(x) contrat(s) résultant(s). En outre, les obligations permanentes en matière de sécurité et de confidentialité qui sont jointes aux clauses du contrat subséquent s'appliquent pendant la durée du contrat, tandis que les exigences de sécurité de la DOC sont évaluées avant l'attribution de l'AMA. Il existe des exigences de sécurité distinctes et uniques qui s'appliquent à l'AMA et aux contrats subséquents.
Q.84 Il ne semble pas y avoir de distinction entre le fournisseur du SaaS et le fournisseur de l'infrastructure d'infonuagique. Les obligations de sécurité à pailer 2 O6, par exemple, sont contrôlées par le fournisseur de services d'infonuagique (FSI).	**R.84** Lorsque le fournisseur de SaaS et le FSI sont distincts, les obligations de sécurité seraient évaluées à tous les niveaux (fournisseur, fournisseur de SaaS et FSI).
Q.85 Pour pailer 2 O8, est-il suffisant de fournir une validation du fournisseur de l'infrastructure d'infonuagique?	**R.85** Les fournisseurs doivent fournir leurs certifications comme indiqué dans la DOC. Dans le cas où le fournisseur qui présente une offre en réponse à la DOC n'est pas le fournisseur d'infrastructure d'infonuagique, le CCC est conscient qu'il peut être difficile d'obtenir une copie des rapports de l'IaaS. Dans ce cas, le fournisseur doit indiquer au CCC quel fournisseur d'infrastructure d'infonuagique il utilise, et fournir les certificats ainsi qu'une lettre indiquant qu'il est un partenaire enregistré auprès du principal fournisseur à grande échelle, car cela indique son niveau d'expertise avec la plate-forme.
Q.86 Pour pailer 2 O12, peut-on se fier à la norme ISO/IEC 27018 du FSI?	**R.86** Le fournisseur du SaaS et la FSI doivent se conformer aux exigences de l'exigence O12.
Q.87 La demande de propositions (annexe B) exige que les exigences de sécurité soient transmises aux sous-traitants, qui incluront le FSI. Si le Canada a déjà conclu un accord avec le FSI, pouvons-nous nous appuyer sur cette obligation contractuelle? Le FSI n'acceptera aucune responsabilité contractuelle envers nous pour les exigences du Canada.	**R.87** Nous avons déjà examiné cette demande à la question 29, dans la modification 004, et notre position reste inchangée.
Q.88 Annexe B, section 5 (vérification de la conformité) et section 12 (vérification de la conformité) - Nous ne pourrons pas fournir ces informations. L'audit est réalisé de manière indépendante par le FSI et les résultats sont partagés avec les clients. Nous ne serons pas en mesure de réaliser un audit de l'environnement du FSI.	**R.88** Se reporter à la réponse à la question 85.
Q.89 Diverses parties de l'appel d'offres demandent la localisation exacte des centres de données. Pour des raisons de sécurité, le FSI ne divulgue pas les emplacements physiques exacts de son infrastructure. Comment pouvons-nous nous conformer à l'exigence?	**R.89** Les informations demandées concernant l'emplacement des centres de données seront fournies au CCC par le biais d'un accord de non-divulgation. Veuillez vous reporter à la question 50, publiée dans la modification 007, qui décrit les mesures prises pour protéger les informations qui ont été divulguées. Si nécessaire, un FSI peut également fournir ces informations directement au CCC par le biais d'un accord de non-divulgation plutôt que de les communiquer au titulaire de l'AMA ou à SPAC.
Q.90 Est-ce votre position actuelle que tous les fabricants d'origine ont besoin de ces éléments pour passer l'évaluation de sécurité : - ASI au niveau Secret - ADR au niveau Protégé B Et ces exigences sont-elles limitées au titulaire de l'OC (volet 3 - revendeurs) ou le titulaire de l'OC et l'éditeur du SaaS doivent-ils également satisfaire à la LVERS?	**R.90** Les niveaux de sécurité suivants sont requis, quel que soit le volet (volet 1 - Protégé B, volet 2 - Protégé A, ou volet 3 - RPM Protégé A) ASI – Protégé B ADR – Protégé B Dans le cadre de l'évaluation du CCC, on exige que le FSI et l'éditeur du SaaS répondent aux exigences de la LVERS (ASI/ADR - Protégé B). En outre, de la

QUESTIONS	RÉPONSES
	manière dont la DOC est actuellement structurée, un RPM qui postule au volet 3 serait également tenu de détenir les habilitations de sécurité industrielle détaillées ci-dessus, car ils sont les titulaires de l'OC.
Q.91 Le Canada peut-il confirmer combien d'accords ont été conclus à ce jour dans le cadre de ce marché?	**R.91** Pour une liste des OC qui ont été attribués à ce jour, veuillez consulter la section Avis d'attribution connexes de la DOC affichée ici : https://achatsetventes.gc.ca/donnees-sur-l-approvisionnement/appels-d-offres/PW-EEM-003-35660.
Q.92 Dans l'annexe A, Qualifications, sous Assurance du volet 1 (jusqu'à et y compris les données de niveau Protégé A), l'exigence de démontrer la conformité pour la colonne de niveau 1 de O7 Gestion des risques de la chaîne d'approvisionnement, l'exigence stipule : Pour être jugée conforme, la documentation fournie doit démontrer la conformité du fournisseur à l'une des trois normes suivantes : 1. ISO/IEC 27036 Technologies de l'information – Techniques de sécurité – Sécurité d'information pour la relation avec le fournisseur (parties 1 à 4); ou 2. publication spéciale 800-161 du NIST – Supply Chain Risk Management Practices for Federal Information Systems and Organizations (pratiques de gestion des risques de la chaîne d'approvisionnement pour les systèmes d'information et organisations du fédéral); ou 3. Catalogue des contrôles de sécurité ITSG-33, sections SA-12 et SA-12(2), où les mesures de sécurité définies et organisées sont documentées dans un plan de gestion des risques de la chaîne d'approvisionnement (GRCA). Le plan de GRCA doit décrire la démarche du fournisseur du logiciel-service en matière de GRCA et démontrer la façon dont le fournisseur du logiciel-service public commercial proposé réduira et atténuera les risques de la chaîne d'approvisionnement. L'État peut-il confirmer qu'elle acceptera les documents d'auto-évaluation pour les trois options afin de justifier l'exigence O7, Gestion des risques de la chaîne d'approvisionnement?	**R.92** Les fournisseurs sont tenus de posséder les homologations ISO 27001, ISO 27017 et SOC 2 de type 2, ainsi que des rapports d'audit complets pour le volet 2. Pour le volet 1, soit ISO 27001, soit SOC 2 de type 2 est requis. Pour le pailer 1 O7 de l'annexe A, les rapports de certification et d'évaluation ne sont pas nécessaires, mais fortement recommandés comme un PSC auto-évalué sera évalué avec un risque plus élevé. Pour le pailer 2 O11, des rapports de certification et d'évaluation sont requis et des preuves pour chaque contrôle sont exigées.
Q.93 Dans les clauses contractuelles de la DOC, il y a une disposition qui permet au fournisseur de faire des représentations (demandes de renseignements) afin d'expliquer pourquoi une clause est trop restrictive. Y a-t-il un document ou un modèle que nous devrions utiliser dans un tel cas, ou une lettre du fournisseur est-elle acceptable? En outre, y a-t-il une date limite dans le processus ou une période particulière pour ces demandes de renseignements? Enfin, s'il existe un tel processus, quel est le délai de réponse?	**R.93** Les fournisseurs peuvent poser des questions et demander des modifications aux conditions de la DOC d'offres et du contrat qui en résulte en soumettant leurs questions par courrier électronique à notre adresse électronique générique : TPSGC.LENQS-SAAS.PWGSC@tpsgc-pwgsc.gc.ca Il n'y a pas de date limite pour poser des questions. Le temps de réponse dépendra de la nature de la question. Dans certains cas, nous devrons consulter d'autres équipes (p. ex., CCC, DSIC/DSII et Services juridiques).
Q.94 Annexe A, volet 1, palier 2 M12 stipule que les documents de certification ISO 27018, qui doivent avoir été délivrés dans les 12 mois précédant la date de soumission, doivent être fournis. Cela signifie-t-il que la norme ISO 27018 doit avoir été délivrée au cours des 12 derniers mois, ou il y a plus de 12 mois?	**R.94** La norme ISO 27018 doit avoir été délivrée dans les 12 mois précédant la date de soumission.
Q.95 S'il n'y a rien à divulguer, est-il nécessaire de présenter un formulaire de déclaration de culpabilité?	**R.95** Non, s'il n'y a rien à divulguer, il n'est pas nécessaire de soumettre un formulaire de déclaration de culpabilité avec votre offre. Les conditions dans lesquelles un formulaire de déclaration de culpabilité doit être soumis sont détaillées au lien suivant :

QUESTIONS	RÉPONSES
	https://www.tpsgc-pwgsc.gc.ca/ci-if/declaration-fra.html
Q.96 Si un client a déjà acheté la solution de SaaS par le biais d'une autre méthode de passation de marché, peut-il utiliser l'OC de SaaS pour le volet des services professionnels uniquement?	**R.96** Oui, il le peut, à condition que la solution soit disponible par le biais de la méthode. Si la solution n'est pas disponible par le biais de la méthode, il devra se procurer des services professionnels pour la solution en dehors de la DOC.
Q.97 Est-il possible que les contrats de SaaS soient pluriannuels?	**R.97** La DOC n'impose aucune limitation de durée de contrat. Cela ne veut pas dire qu'un client n'aurait pas de contraintes ministérielles ou autres, mais la DOC elle-même ne contient aucune restriction concernant la durée du contrat ou les années d'option.
Q.98 Section 4.1, Services de la solution e) Octroi des droits d'utilisation. L'entrepreneur accorde au Canada le droit d'accéder à la solution et de l'utiliser sur une base non exclusive et incessible, à partir d'un nombre illimité d'emplacements, d'appareils et d'environnements d'exploitation, au moyen d'une connexion sécurisée, sans fil, mobile ou autre, au moyen d'un navigateur Web ou d'une autre technologie de connexion qui pourrait devenir disponible. Cela signifie-t-il que des licences gratuites illimitées sont attendues?	**R.98** La section 4.1(e) des modalités du contrat résultant ne stipule pas que des licences illimitées doivent être fournies, mais plutôt que la solution doit être disponible pour une utilisation sur un nombre illimité d'emplacements, de dispositifs et d'environnements d'exploitation. C'est le droit d'accès et d'utilisation de la solution qui est en question ici, et non le nombre de licences à fournir.
Q.99 Nous travaillons avec plusieurs ministères au sein du gouvernement, et notre modèle de tarification est personnalisé pour répondre aux besoins de chaque ministère. Nous n'avons pas de structure tarifaire standard. Comment ce processus affectera-t-il la tarification et les contrats actuellement en vigueur?	**R.99** Le processus de DOC aura aucune effet sur les contrats actuellement en vigueur. Pour savoir comment préparer l'annexe C - Catalogue de Solutions de logiciels-services et Prix Plafonds, veuillez consulter la partie 3.3, section II : Soumission financière.
Q.100 En ce qui concerne le volet 1, M7 - Gestion des risques de la chaîne d'approvisionnement, SPAC confirmera-t-il que si un fournisseur peut démontrer l'harmonisation sur au moins une de ces options au moyen d'un questionnaire d'auto-évaluation avec attestation, il sera considéré comme conforme à l'exigence?	**R.100** Se reporter à la réponse à la question 92.
Q.101 Nous demandons que l'on envisage de modifier le texte de l'annexe F, Clauses du contrat subséquent, section 3.5, comme suit : Si l'entrepreneur n'est pas en mesure de fournir les services avec des caractéristiques et des fonctionnalités non moins favorables, il doit en aviser le Canada par écrit en précisant les circonstances et les autres options possibles, notamment une réduction du prix. Si aucune option de rechange proposée n'est acceptable pour le Canada, l'entrepreneur consent à une résiliation du contrat conformément à la section 7.5.3(c)b.(ii).	**R.101** Cette demande est acceptée et les changements sont reflétés dans la version mise à jour de l'annexe F mentionnée à la section 8.0 de la présente modification ci-dessous.
Q.102 Nous demandons que l'on envisage de modifier le texte de l'annexe F, Clauses du contrat subséquent, section 7.6(b), comme suit : L'entrepreneur convient que, si le Canada demande des services de migration ou de transition pendant la période précédant la fin de la durée du contrat, il aidera de manière raisonnable le Canada à faire la transition entre le présent contrat et le nouveau contrat ou à faire migrer les données du Canada à l'environnement du nouveau fournisseur. Il convient que les services décrits ci-dessous ne donneront lieu à aucuns frais autres que ceux qui sont prévus dans la base de paiement.	**R.102** Cette demande est acceptée et les changements sont reflétés dans la version mise à jour de l'annexe F mentionnée à la section 8.0 de la présente modification ci-dessous.

3.0 Journée de l'industrie – questions et réponses :

Remarque : les questions peuvent avoir été modifiées ou résumées.

JOURNEE DE L'INDUSTRIE QUESTIONS	JOURNEE DE L'INDUSTRIE RÉPONSES
JIQ.20 Cette méthode sera-t-elle utilisée pour acquérir des services professionnels également, ou encore cette méthode vise-t-elle principalement à obtenir des solutions de logiciels-services?	**JIR.20** Cette méthode visera à acquérir des solutions de logiciels-services et des services professionnels connexes. Lorsque vous présentez l'annexe C, vous pouvez y inclure les services professionnels; la portée de ceux-ci doit toutefois s'appliquer uniquement aux solutions de logiciels-services vendus au moyen de cette méthode. La section 3.3(b) de la DAMA fait état des types de services professionnels qui peuvent être acquis au moyen de la méthode. Il s'agit notamment de la trousse de formation et de services du Guide de démarrage rapide (GDR), services de mise en œuvre, des services de formation, du nettoyage des données, des services de migration et de transition, ainsi que des services consultatifs.
JIQ.21 SPAC souhaiterait-il que les solutions de plateformes-services s'appliquent dans le cadre de la présente DAMA?	**JIR.21** La DAMA s'applique uniquement aux solutions de logiciels-services (SaaS). On ne peut pas appliquer de solutions de plateformes-services dans le cadre de la présente DAMA.
JIQ.22 Dans quel ordre évaluera-t-on les soumissions présentées au Centre canadien pour la cybersécurité (CCC), c.-à-d. les premiers candidats de la deuxième vague seront-ils traités en premier?	**JIR.22** Le CCC intégrera les candidats. Ensuite, toutes les soumissions seront envoyées à leurs coordonnateurs, qui demanderont tout document supplémentaire pour faciliter le processus d'évaluation. L'ordre d'évaluation d'un fournisseur sera déterminé une fois qu'il fournira tous les documents nécessaires. Par conséquent, ce n'est pas nécessairement l'ordre dans lequel leur soumission a été intégrée, mais plutôt l'ordre dans lequel tous les documents nécessaires ont été reçus aux fins de préparation de la réunion de lancement et d'application du processus d'évaluation.
JIQ.23 Combien de temps le processus d'évaluation du CCC est-il censé durer pour l'évaluation de chaque solution de services infonuagiques présentée?	**JIR.23** À compter de la réunion de lancement, dans le cadre de laquelle le fournisseur décrit les services qu'il propose au CCC, il s'écoule habituellement de 3 à 5 mois; cela dépend toutefois de la quantité de renseignements fournis et de la mesure dans laquelle le fournisseur peut faire preuve de souplesse.
JIQ.24 Les mises à jour de la matrice de traçabilité du Profil des mesures de sécurité pour les services du GC (c.-à-c. contrôles de sécurité de l'ITSG-33) peuvent-elles être présentées pendant le processus d'évaluation du CCC?	**JIR.24** Le CCC a besoin de preuves sous forme de politiques et de procédures pour les contrôles, de manière à s'assurer qu'on s'y conforme. Si vous disposez de politique et de procédures dont vous pouvez faire part au CCC, vous pouvez les ransmette pendant le processus d'intégration. Autrement, le CCC assurera un suivi des politiques et des procédures pendant le processus d'évaluation.
JIQ.25 Certaines composantes de solutions infonuagiques peuvent nécessiter le soutien de ressources techniques de l'extérieur du Canada (p. ex., soutien de niveau 3). La prestation d'un tel soutien sera-t-elle permise et y a-t-il des exigences supplémentaires relatives à la sécurité ou une procédure particulière d'accès à distance qui devra être suivie? Ces ressources devront-elles détenir des attestations de sécurité du personnel du GC?	**JIR.25** Si du personnel au Canada doit avoir accès à des renseignements protégés, celui-ci devra obtenir une cote de fiabilité, sauf s'il est déterminé qu'il s'agit d'un utilisateur administratif ou privilégié, ce qui nécessiterait une attestation de sécurité de niveau secret À l'échelle internationale, cela peut être autorisé, mais l'organisation étrangère serait tenue de passer par le processus de d'évaluation de sécurité. Pour obtenir une équivalence du statut de fiabilité, l'entreprise doit fournir certaines preuves, y compris, mais sans s'y limiter, un formulaire d'attestation, un formulaire de vérification des antécédents, un DSC rempli et des listes de vérification informatiques. Pour obtenir une équivalence de statut secret, le fournisseur étranger doit être situé dans un pays qui a conclu un accord bilatéral avec le Canada (voir le lien

JOURNEE DE L'INDUSTRIE QUESTIONS	JOURNEE DE L'INDUSTRIE RÉPONSES
	ci-dessous pour une liste de ces pays). Dans ces cas, le fournisseur étranger devrait obtenir l'assurance de l'autorité nationale de sécurité de ce pays, et cela pourrait prendre jusqu'à un an. https://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html
JIQ.26 Pouvez-vous confirmer comment l'on traitera les produits/fournisseurs existants de logiciels-services qui ont déjà été certifiés dans le cadre du Programme de sécurité du CCC/SPAC pour les renseignements jusqu'au niveau Protégé B?	**JIR.26** Si vous avez déjà participé au processus de DAMA de SPAC dans le cadre de la vague 1 du CCC, il n'est pas nécessaire de présenter une nouvelle demande. Si vous avez été évalué par le CCC dans le cadre d'une autre méthode, vous pourriez tout de même présenter une demande pour la vague 2. Si vous avez déjà été évalué par le CCC, vous devez présenter le rapport sommaire que ce dernier vous a fourni. Le CCC intégrera ensuite le fournisseur au programme, s'assurera qu'il n'y a eu aucun changement, et que les mêmes produits ont été évalués. Dans le cadre du Programme de sécurité des contrats, vous devez détenir les attestations de sécurité et la documentation précisées dans la DAMA (annexe G ou H). Si vous avez obtenu les attestations et la documentation indépendamment de la méthode, ou si vous vous êtes déjà conformé aux exigences de sécurité de la DSIC ou la DSII et détenez déjà votre vérification d'organisation désignée (VOD), votre autorisation de détenir des renseignements (ADR) ou des attestations de sécurité du personnel, vous n'auriez pas à faire l'objet du processus de nouveau. Il faudrait que les attestations soient confirmées auprès de la DSIC ou de la DSII, selon le cas.
JIQ.27 Combien de temps le processus auprès du CCC est-il censé durer?	**JIR.27** Le processus d'intégration auprès du CCC s'échelonne sur quelque 28 jours. Vous recevrez un courriel environ une semaine suivant votre intégration. La réunion de lancement avec le CCC devrait avoir lieu peu après. À la suite de la réunion de lancement, il s'écoulera à peu près trois à cinq mois, ce qui comprend également le processus d'évaluation de l'intégrité de la chaîne d'approvisionnement.
JIQ.28 Comment pouvons-nous déterminer les plateformes qui ont été évaluées par le CCC?	**JIR.28** Ces plateformes sont indiquées sur le site Web du Service de courtage infonuagique (https://cloud-broker.canada.ca/s/central-provider-page-v2?language=fr). Si vous êtes hébergé sur votre propre plateforme, le CCC peut évaluer cet aspect également, ce qui pourrait prendre un peu plus de temps, car il s'agir d'un composant complet qui nécessitera davantage d'éléments de sécurité physique.
JIQ.29 Quelle est la procédure à suivre pour faire signer une entente de non-divulgation (END)?	**JIR.29** Même si la vague 2 est ouverte, veuillez communiquer par courriel à l'adresse contact@cyber.gc.ca. Le CCC entamera le processus d'END une fois que vous aurez communiqué avec lui. Le CCC enverra également une trousse de présentation et une clé PGP. Si vous ne souhaitez pas utiliser une clé PGP, ce dernier recommande d'utiliser la protection par de mot de passe pour l'envoi de tout document.

JOURNEE DE L'INDUSTRIE QUESTIONS	JOURNEE DE L'INDUSTRIE RÉPONSES
JIQ.30 Pouvez-vous confirmer qu'une attestation de sécurité d'installation de niveau secret) est requise pour les organisations qui proposent des solutions uniquement dans le volet Protégé A?	**JIR.30** En ce qui a trait à une organisation qui a accès à des renseignements protégés, une VOD sera entamée et accordée à son intention. Une ASI est requise pour accéder à des renseignements classifiés; une telle attestation ne serait donc pas accordée à une organisation. Cependant, l'agent de sécurité d'entreprise et certains utilisateurs privilégiés qui seront identifiés auront besoin d'une attestation de niveau secret. Dans le cadre du Programme de sécurité des contrats, un processus en place permettra au personnel d'obtenir une attestation de niveau secret, même si l'organisation en question détient uniquement un VOD.
JIQ.31 Pouvez-vous expliquer en quoi un fournisseur d'applications-services et un fournisseur de services infonuagiques diffèrent dans le contexte de la présente DAMA?	**JIR.31** Le fournisseur d'applications-services et le fournisseur de services infonuagiques peuvent être identiques, mais si la solution de logiciels-services est hébergée sur le nuage d'un tiers, il y aura une différence. Sur le plan de la sécurité, le CCC recommande de faire appel à un fournisseur de services infonuagiques, à un logiciel-service et à une solution de plateformes-ayant déjà été évalués. Autrement, le CCC serait tenu d'évaluer le fournisseur de logiciels-services lui-même, car certains contrôles peuvent être transmis et le CCC a besoin de comprendre en quoi consistent les composantes ayant été transmises.
JIQ.32 Un éditeur de logiciels-services peut-il attribuer plus d'un utilisateur privilégié?	**JIR.32** À l'heure actuelle, il n'y a pas de limite quant au nombre d'administrateurs ou d'utilisateurs privilégiés qu'un éditeur de logiciels-services peut attribuer. Une limite pourrait toutefois être fixée ultérieurement.
JIQ.33 Y a-t-il des exigences particulières relatives à la sécurité pour les entreprises canadiennes travaillant avec des équipes de TI éloignées?	**JIR.33** Toutes les entreprises seraient tenues de respecter les exigences relatives à la sécurité du contrat. Des exigences supplémentaires s'appliqueraient lorsqu'il s'agirait de faire appel à des ressources étrangères. En ce qui a trait à la cote de fiabilité, la preuve d'équivalence est requise, ce qui peut prendre jusqu'à cinq jours. Les rôles assortis d'un accès privilégié nécessiteraient une attestation de niveau secret ou l'équivalent, ce qui peut prendre jusqu'à un an, du fait qu'il faut passer par l'autorité de sécurité du pays en question.
JIQ.34 Pouvez-vous préciser le processus concernant l'exigence de détenir une autorisation de détenir des renseignements pour les entreprises qui présentent une demande liée au niveau Protégé A?	**JIR.34** Après l'approbation de l'attestation de vérification d'organisation désignée (VOD), l'équipe du Programme de sécurité des contrats communiquera avec l'agent de sécurité de l'entreprise (ASE) pour confirmer la nature de la présence au Canada et l'endroit où l'information est hébergée (que ce soit dans votre installation ou dans une autre installation qui a déjà été évaluée et approuvée). Par la suite, on déterminera les exigences nécessaires. Nous ne pouvons pas donner de détails sur les exigences, car chaque entreprise et chaque site sont différents.
JIQ.35 Un déploiement dans des locaux existants justifie-t-il le recours à un fournisseur unique d'une solution équivalente à la solution de logiciel-service (c.-à-d. une migration vers des logiciels-services)? Qu'en est-il s'il est possible d'utiliser une licence personnelle pour réduire les coûts de paiement à l'utilisation des logiciels-services?	**JIR.35** Il ne s'agirait pas d'une justification de fournisseur unique suffisante. Un modèle d'utilisation de licence personnelle ne serait acceptable dans ce cas, car la seule chose permise dans la DAMA est la solution de logiciel-service (SaaS). Dans un modèle d'utilisation de licence personnelle, le client possède déjà ses propres licences; il ne ferait pas nécessairement l'acquisition d'un logiciel-service, il hébergerait plutôt ses licences existantes, alors cela ne s'appliquerait pas.

JOURNEE DE L'INDUSTRIE QUESTIONS	JOURNEE DE L'INDUSTRIE RÉPONSES
JIQ.36 Comment SPAC et Services partagés Canada (SPC) coordonnent-ils leurs activités pour s'assurer que le gouvernement du Canada (GC) dispose des meilleures solutions et que les normes sont respectées?	**JIR.36** Pour ce qui est des normes, les exigences en matière de sécurité infonuagique sont les mêmes à l'échelle du GC. Pour ce qui est du chevauchement des produits accessibles, ce serait aux ministères clients de déterminer la voie à suivre s'il était possible d'avoir recours à deux mécanismes d'approvisionnement pour la même solution. Nous ne pouvons pas faire de commentaires sur ce qui est accessible par l'entremise de SPC; cependant, nous pouvons dire que nous avons fait part de la DAMA à SPC, qui a été informé du processus de demande, de la façon dont les ministères peuvent y accéder, de l'évaluation menée par le Centre canadien pour la cybersécurité (CCC) ainsi que des exigences de la DAMA.
JIQ.37 Existe-t-il une liste de pays avec lesquels le Canada a conclu des ententes facilitant le processus d'habilitation de sécurité pour le personnel à l'étranger?	**JIR.37** La liste des pays qui ont conclu un accord de sécurité bilatéral avec le Canada se trouve dans le lien suivant: https://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html
JIQ.38 En tant que fournisseur d'une solution de logiciel-service, nous ne fournissons pas directement les services nécessaires à la mise en place du logiciel. Nous comptons sur un vaste réseau de partenaires qui mettent en place notre logiciel et le personnalisent en fonction des besoins de l'organisation. Nos partenaires qui s'occupent de cette mise en place doivent-ils également se qualifier dans le cadre du processus de DAMA?	**JIR.38** Vous pouvez énumérer les services professionnels qui ne sont pas offerts par le fournisseur de la solution de logiciel-service, mais s'il y avait des exigences en matière de sécurité du personnel qui doivent être satisfaites relativement à ces services professionnels, alors on procéderait à une évaluation, et les exigences devraient être respectées par l'entreprise qui offre ces services. Le fournisseur de solution de logiciel-service serait responsable de veiller à ce que les exigences du contrat soient respectées dans le cadre de la prestation du travail visé, ce qui nécessiterait normalement l'établissement d'une entente ou d'un contrat de sous-traitance distinct avec ces entreprises.
JIQ.39 En ce qui concerne les fournisseurs de services infonuagiques qui sont déjà certifiés, la certification vise-t-elle seulement les régions du Canada où ils se trouvent? Ou s'applique-t-elle aussi à d'autres régions?	**JIR.39** Seules les régions canadiennes ont été évaluées, car certains fournisseurs de services infonuagiques mettent en œuvre des éléments différents selon le pays d'origine.
JIQ.40 Quelle sera la limite liée à un fournisseur unique dans le cadre du véhicule en question?	**JIR.40** Le véhicule ne prévoit pas de limite dans le cas d'un fournisseur unique indépendant. Quiconque effectue un achat de plus de 40 000 $ par l'entremise du véhicule serait tenu de présenter une justification du recours à un fournisseur unique pour traiter directement avec une entreprise. Pour un achat de moins de 40 000 $, on pourrait contacter directement une entreprise en particulier sans justification de recours à un fournisseur unique. Il est également important d'ajouter que les ministères clients, lorsqu'il est question de ce point, n'auront pas nécessairement à fournir cette justification à SPAC s'ils font un achat en vertu de leur pouvoir délégué, mais ils devront la consigner dans leurs propres dossiers internes. Si le marché dépasse les pouvoirs qui lui ont été délégués, ou dans tous les cas où SPAC effectue l'approvisionnement en son nom, le ministère devra fournir à SPAC sa justification de fournisseur unique, qui sera examinée et validée avant qu'on aille de l'avant avec l'approvisionnement.
JIQ.41 Si une procédure de gestion d'urgence est en place, devons-nous quand même passer par le processus d'autorisation de sécurité pour les ressources de soutien à l'extérieur du Canada?	**JIR.41** Il faudrait alors entamer le processus d'autorisation de sécurité pour les ressources de soutien à l'extérieur du Canada. Si elles disposent déjà d'une attestation de sécurité, une vérification à cet égard devra être faite.

JOURNEE DE L'INDUSTRIE QUESTIONS	JOURNEE DE L'INDUSTRIE RÉPONSES
JIQ.42 À quoi peut-on s'attendre à l'avenir en ce qui concerne les besoins en logiciels sur place? L'arrangement en matière d'approvisionnement concernant les licences de logiciels (AALL) demeurera-t-il en place?	**JIR.42** L'AALL reste en place et est indépendant de la DAMA, car les logiciels sur place représenteront un besoin continu pour le GC dans un avenir prévisible. Les deux véhicules seront mis à la disposition des ministères clients, et les clients qui ont besoin d'un logiciel sur place seront en mesure d'utiliser l'AALL ou d'effectuer des achats dans un cadre autre que celui de l'AALL.
JIQ.43 En ce qui a trait à la certification de niveau Protégé B, faut-il qu'il y ait un ASE canadien (personne vivant au Canada)?	**JIR.43** Pour que l'organisation canadienne reçoive une attestation de sécurité, l'ASE doit être un citoyen canadien ou un résident permanent et résider au Canada. Tous les super-utilisateurs ou utilisateurs privilégiés de l'organisation que nous inscrivons au programme doivent également être des employés de l'organisation qui est inscrite, et non des employés d'une société mère.
JIQ.44 Quelle est la prochaine période prévue par le CCC après celle visée?	**JIR.44** À ce stade-ci, aucune date exacte n'est définie pour ce qui est de la prochaine période. Le CCC examinera les demandes de la vague 2 avant de déterminer la date de la prochaine période.
JIQ.45 Voulez-vous que les fournisseurs obtiennent d'abord les approbations de niveau Protégé A, afin de réduire les efforts en vue du passage au niveau Protégé B par la suite (p. ex., si nous avons d'autres audits concernant les certifications ISO/SOC2 en cours)? Ou devrions-nous simplement attendre et entreprendre le processus lié au niveau Protégé B plus tard en partant de zéro?	**JIR.45** Cette décision revient aux fournisseurs. Si vous n'avez pas de solutions pour les données de niveau Protégé A, nous vous recommandons d'attendre et de faire le processus lié au niveau Protégé B lorsque vous serez prêt. La capacité d'évaluation des solutions du CCC étant limitée, nous ne voulons pas qu'il fasse une évaluation du niveau Protégé A si cela n'est pas utile pour les clients.
JIQ.46 Si un ministère souhaite obtenir une solution de logiciel-service pour des besoins de nature non classifiée, doit-il quand même obtenir l'approbation pour le niveau Protégé A?	**JIR.46** Comme le niveau le plus bas visé par la DAMA est Protégé A, il est nécessaire de se qualifier pour le niveau Protégé A. Autrement, l'approvisionnement pour une solution de nature non classifiée devrait se faire autrement que par l'intermédiaire de la DAMA; il est toutefois important de noter qu'il y aurait encore des exigences de sécurité à évaluer dans un tel scénario. Il peut être difficile pour les ministères clients d'effectuer eux-mêmes une évaluation de l'intégrité de la chaîne d'approvisionnement et de la sécurité des TI de niveau inférieur. On a mis la DAMA en place afin de simplifier ce processus pour les ministères clients, et bien que ceux-ci puissent faire des achats de niveau non classifié au moyen d'un véhicule autre que la DAMA, nous encourageons les fournisseurs à se qualifier dans le cadre de la DAMA et les ministères clients à faire des achats par l'entremise de celle-ci dans la mesure du possible, étant donné que la plupart des ministères clients s'emploient encore à renforcer leur capacité à effectuer ces évaluations eux-mêmes. Comme le CCC accorde la priorité aux véhicules d'approvisionnement relatif au nuage du GC, y compris la présente DAMA, il s'agit d'une méthode à utiliser de préférence par les clients.
JIQ.47 En ce qui concerne les exigences de qualification énumérées à l'annexe A de la DAMA, si une soumission ne comprend pas de rapports d'audit complets pour toutes les attestations énumérées, est-elle immédiatement exclue?	**JIR.47** Si vous n'avez que les attestations et non les rapports d'audit complets, vous ne ferez pas partie de l'intégration, car le CCC a besoin de ces rapports pour effectuer l'évaluation. Lorsque vous soumettez une demande à l'équipe de la DAMA de SPAC, et non pendant une période d'intégration du CCC, vous pouvez nous présenter tous les documents et formulaires requis sans ces attestations. Ce n'est que lorsqu'on vous intégrera au processus d'évaluation de la sécurité des TI du CCC que vous aurez besoin de ces attestations et de ces rapports d'audit.

4.0 Annexe A pailer 1 O5 et O7, et palier 2 O8 et O11, est par les présentes supprimée et remplacée par le suivant:

ID de l'exigence obligatoire	Sous-catégorie	Exigence	Obligation de démontrer la conformité au palier 1 (données jusqu'au niveau Protégé A, inclusivement)
O5	**Assurance d'une tierce partie**	Le logiciel-service doit être conçu et développé pour assurer la sécurité de leur logiciel-service public proposé disponible sur le marché, y compris la mise en œuvre des politiques, des procédures et des contrôles de sécurité de l'information. Pour les fournisseurs qui ont déjà complété l'évaluation en sécurité en fournissant au CCC les rapports de certification de sécurité SOC 2 Type II et qui ont déjà conclu une entente de non divulgation (END) avec le CCC doivent transmettre leur certification et leurs rapports de certification directement au CCC à contact@cyber.gc.ca afin de se conformer à cette exigence. Pour les fournisseurs qui n'ont pas complété l'évaluation en sécurité, le processus d'intégration commencera une fois que la soumission respectera les exigences de la demande d'arrangement en matière d'approvisionnement et satisfera à tous les critères d'évaluation techniques et financiers obligatoires et fournira tous les éléments obligatoires de certifications pour être déclarée recevable. SPAC référera ensuite le fournisseur aux services clients de CCC pour commencer le processus d'intégration de l'évaluation en TI et pour conclure une END en vue de recevoir une copie du formulaire de soumission d'intégration, ainsi que toute information supplémentaire exigée aux termes de cette exigence.	Le fournisseur doit présenter une documentation au Canada démontrant la façon dont le fournisseur du logiciel-service public commercial respecte les exigences relatives l'assurance d'une tierce partie. La conformité doit être démontrée par la présentation d'au moins une des certifications de l'industrie énoncées ci-dessous, puis validée au moyen d'évaluations de tiers indépendants. Le fournisseur doit présenter les certifications et rapport d'évaluations suivantes de l'industrie afin de démontrer la conformité du service proposé : (a) l'une des certifications suivantes : (i) ISO/IEC 27001:2013 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences, (ii) contrôle de l'organisation des services (SOC) de l'AICPA – rapports des SOC 2 de type II; (b) autoévaluation de ses services par rapport à la version 3.01 (ou une version ultérieure) de la matrice des contrôles infonuagiques (MC) de la Cloud Security Alliance (CSA). Chaque rapport de certification et d'évaluation fourni doit : 1. être valide à la date de clôture de la soumission, 2. indiquer la dénomination sociale du fournisseur proposé et du sous-traitant du fournisseur, s'il y a lieu, y compris le fournisseur de services infonuagiques, 3. indiquer la date ou l'état de la certification actuelle, 4. comprendre la liste des biens, de l'infrastructure du fournisseur et des emplacements de service dans le cadre du rapport de certification,

ID de l'exigence obligatoire	Sous-catégorie	Exigence	Obligation de démontrer la conformité au palier 1 (données jusqu'au niveau Protégé A, inclusivement)
			5. indiquer les emplacements et les services offerts par le fournisseur proposé. Si la méthode déterminée est utilisée pour exclure les organisations de services en sous-traitance, comme l'hébergement de centres de données, le rapport d'évaluation de l'organisation sous-traitante doit être inclus, et 6. être délivré par un tiers indépendant qualifié au titre de l'AICPA ou de CPA Canada ou du régime de certification ISO, et respecter la norme ISO/IEC 17020 relativement aux systèmes de gestion de la qualité. **Remarque** : • Les certifications doivent être fournies pour toutes les parties du service proposé. • Les certifications doivent être accompagnées de rapports d'évaluation. • Les certifications doivent être valides et avoir été émises dans les 12 mois précédant le début du contrat.
O7	**Gestion des risques de la chaîne d'approvisionnement**	Le fournisseur du logiciel-service public commercial proposé doit mettre en œuvre des mesures de protection afin de réduire les vulnérabilités de la chaîne d'approvisionnement des services de TI et les menaces qui la guettent. En font notamment partie la conception et la mise en œuvre de contrôles visant à atténuer et à contenir les risques liés à la sécurité des données par une séparation adéquate des tâches, un accès établi selon les fonctions des utilisateurs et un accès qui suit le principe du privilège minimal pour tout le personnel au sein de la chaîne d'approvisionnement.	Le fournisseur doit démontrer la façon dont le fournisseur du logiciel-service public commercial respecte les exigences, comme le précise le programme d'évaluation de la sécurité de la technologie de l'information du fournisseur du logiciel-service. Pour être jugée conforme, la documentation fournie doit démontrer la conformité du fournisseur à l'une des trois normes suivantes : 1. ISO/IEC 27036 Technologies de l'information – Techniques de sécurité – Sécurité d'information pour la relation avec le fournisseur (parties 1 à 4); ou 2. publication spéciale 800-161 du NIST – *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (pratiques de gestion des risques de la chaîne

ID de l'exigence obligatoire	Sous-catégorie	Exigence	Obligation de démontrer la conformité au palier 1 (données jusqu'au niveau Protégé A, inclusivement)
			d'approvisionnement pour les systèmes d'information et organisations du fédéral); ou 3. Catalogue des contrôles de sécurité ITSG-33, sections SA-12 et SA-12(2), où les mesures de sécurité définies et organisées sont documentées dans un plan de gestion des risques de la chaîne d'approvisionnement (GRCA). Le plan de GRCA doit décrire la démarche du fournisseur du logiciel-service en matière de GRCA et démontrer la façon dont le fournisseur du logiciel-service public commercial proposé réduira et atténuera les risques de la chaîne d'approvisionnement. ou 4. contrôles CSA STAR pour soutenir les contrôles de gestion de la chaîne d'approvisionnement CSA CCM

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O8	**Assurance d'une tierce partie**	Le logiciel sous forme de service commercialement disponible doit être conçu et élaboré pour garantir la sécurité du logiciel-service commercialement disponible proposé et comprendre la mise en oeuvre de politiques et de procédures sur la sécurité de l'information et de mesures de contrôle de la sécurité. Le fournisseur du logiciel-service commercialement disponible proposé doit également se conformer aux exigences de sécurité sélectionnées dans le Profil des mesures de sécurité pour les services de la TI du GC fondés sur l'informatique en nuage pour les renseignements classés « Protégés B, intégrité moyenne, disponibilité moyenne »	Le fournisseur doit démontrer comment le fournisseur du logiciel-service commercialement disponible proposé se conforme aux exigences de la rubrique Exigences relatives à l'assurance des tiers. La conformité doit être démontrée par la mise en correspondance des contrôles de sécurité avec les certifications de l'industrie applicables énoncées ci-dessous, puis validée au moyen d'évaluations de tiers indépendants. Le fournisseur doit fournir chacune des certifications et rapport d'évaluation suivantes de l'industrie pour démontrer sa conformité : 1. ISO/IEC 27001:2013 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
		(PBMM) pour la portée du logiciel-service commercialement disponible proposé fourni. La conformité sera validée et vérifiée au moyen du processus d'évaluation de la sécurité des technologies de l'information (TI) du fournisseur de services infonuagiques (CSP) du Centre canadien pour la cybersécurité (CCCS) (ITSM.50.100) (https://cyber.gc.ca/fr/orientation/processus-devaluation-de-la-securite-des-technologies-de-linformation-sappliquant-aux). Tout fournisseur qui a participé au processus doit fournir de la documentation confirmant qu'il a terminé le processus d'intégration avec (i) une copie du plus récent rapport d'évaluation rempli fourni par le CCCS; et (ii) une copie du rapport sommaire le plus récent fourni par le CCCS. Cela accélérera le processus de qualification et, en même temps, n'oblige pas le fournisseur à démontrer la conformité. Pour les fournisseurs qui ont déjà complété l'évaluation en sécurité en fournissant au CCC les rapports de certification de sécurité SOC 2 Type II et qui ont déjà conclu une entente de non divulgation (END) avec le CCC doivent transmettre leur certification et leurs rapports de certification directement au CCC à contact@cyber.gc.ca afin de se conformer à cette exigence. Pour les fournisseurs qui n'ont pas complété l'évaluation en sécurité, le processus d'intégration commencera une fois que la soumission respectera les exigences de la	2. ISO/IEC 27017:2015 Technologies de l'information – Techniques de sécurité – Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage 3. AICPA Service Organisation Control (SOC) 2 de type II pour les principes de confiance de sécurité, de disponibilité, d'intégrité du traitement et de confidentialité. Chaque certification et rapport d'évaluation doit : (a) être valide à la date de clôture de la demande de soumissions; (b) indiquer la raison sociale légale du fournisseur du logiciel-service commercialement disponible proposé et du fournisseur de services d'informatique en nuage; (c) indiquer la date ou l'état de la certification actuelle; (d) donner la liste des actifs, de l'infrastructure du fournisseur et des emplacements de service dans le cadre du rapport de certification; (e) la portée du rapport doit renvoyer aux lieux et aux services proposés par le logiciel sous forme de service commercialement disponible proposé. Si la méthode créée est utilisée pour exclure les organisations de sous-services comme la prise en charge de centres de données, le rapport d'évaluation de l'organisation de sous-services doit être joint; et (f) être délivré par un tiers indépendant certifié en vertu de l'American Institute of Certified Public Accountants (AICPA) ou de CPA Canada (Comptables professionnels agréés du Canada) ou encore du régime de certification ISO, et être conforme à la norme ISO/IEC 17020 sur les systèmes de gestion de la qualité. Le fournisseur peut fournir des renseignements supplémentaires tirés de plans de sécurité du système, de documents de conception de système d'information, de documents d'architecture de système d'information ou de documents qui

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
		demande d'arrangement en matière d'approvisionnement et satisfera à tous les critères d'évaluation techniques et financiers obligatoires et fournira tous les éléments obligatoires de certifications pour être déclarée recevable. SPAC référera ensuite le fournisseur aux services clients de CCC pour commencer le processus d'intégration de l'évaluation en TI et pour conclure une END en vue de recevoir une copie du formulaire de soumission d'intégration, ainsi que toute information supplémentaire exigée aux termes de cette exigence.	donnent une description détaillée du système, comme l'évaluation de ses services conformément à la version 3.01 de la Cloud Controls Matrix (CCM) de la Cloud Security Alliance (CSA) ou à une version subséquente, pour complémenter les allégations de certifications ci-dessus, afin de démontrer la conformité au Profil des mesures de sécurité pour les services de la TI du GC fondés sur l'informatique en nuage pour les renseignements classés Protégé B, intégrité moyenne et disponibilité moyenne (PBMM). **Remarque :** • Des certifications doivent être fournies pour toutes les parties des services proposés. • Les certifications doivent être accompagnées de rapports d'évaluation.
O11	**Gestion des risques de la chaîne d'approvisionnement**	Le fournisseur du logiciel-service commercialement disponible proposé doit prendre des mesures de sécurité pour atténuer les menaces et les vulnérabilités associées à la chaîne d'approvisionnement des services de TI en vue de préserver la confiance en ce qui concerne la sécurité des sources des systèmes d'information et les composants de TI servant à offrir les services. En font notamment partie la conception et la mise en œuvre de contrôles visant à atténuer et à contenir les risques liés à la sécurité des données par une séparation adéquate des tâches, un accès établi selon les fonctions des utilisateurs et un accès qui suit le principe du privilège minimal pour tout le personnel au sein de la chaîne d'approvisionnement.	Le fournisseur doit démontrer en quoi le fournisseur du logiciel disponible dans le commerce proposé en tant que service est conforme aux exigences des exigences de gestion des risques de la chaîne logistique décrites dans le programme d'évaluation de la sécurité des technologies de l'information des fournisseurs. Pour être considérée comme conforme, la documentation fournie doit démontrer que l'approche de gestion des risques de la chaîne d'approvisionnement utilisée dans le commerce comme logiciel disponible dans le commerce s'aligne sur l'une des meilleures pratiques suivantes. 1. ISO / CEI 27036 Technologies de l'information - Techniques de sécurité - Sécurité de l'information pour les relations avec les fournisseurs (parties 1 à 4); ou 2. Publication spéciale NIST 800-161 - Pratiques de gestion des risques de la chaîne d'approvisionnement pour les systèmes et organisations d'information fédéraux; ou 3. Contrôle de sécurité ITSG-33 pour SA-12 et SA-12 (2) lorsque les garanties de sécurité définies sont documentées dans un plan de gestion des risques liés à la chaîne logistique. Le plan de SCRM doit décrire l'approche du fournisseur en matière de SCRM et indiquer comment les fournisseurs du logiciel-service proposé dans le commerce proposé réduiront et atténueront les risques inhérents à la chaîne d'approvisionnement; ou

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
			4. contrôles CSA STAR pour soutenir les contrôles de gestion de la chaîne d'approvisionnement CSA CCM. Le plan SCRM doit être évalué et validé de manière indépendante par un tiers indépendant certifié selon le régime de certification AICPA ou CPA Canada et / ou ISO. Les fournisseurs doivent indiquer où trouver le matériel de référence, y compris le titre du document, ainsi que les numéros de page et de paragraphe.

5.0 Annexe C - Prix plafonds pour les Solutions de logiciels services et les services professionnels est par les présentes supprimée dans son intégralité et remplacée par le suivant :

Annexe C – Prix plafonds pour les Solutions de logiciels services et les services professionnels

Option 1: Le fournisseur a la possibilité de soumettre les prix plafonds comme indiqué dans le tableau, ou de soumettre la liste de prix commerciaux publiée (par exemple, lien vers un site Web),
Lien vers un site Web :

OU

Option 2: Ce formulaire doit être rempli et soumis dans le cadre de la réponse du fournisseur à la DAMA, si aucun lien n'est fourni dans l'option 1.

TABLEAU 1 – LISTE DE PRODUITS ET PRIX PLAFONDS

Nº d'article	No de pièce de l'éditeur de la Solution de logiciels-services (A)	Nom de la solution de logiciels-services (B)	Nom de l'éditeur de la Solution de logiciels-services (C)	Nom du fournisseur de services infonuagique (D)	Prix plafonds pour les Solutions de logiciels-services (E)	Prix plafonds pour les services professionnels facultatifs (F)	Unité de mesure (G)	Remise en pourcentage applicable (H)	Langue(s) disponible(s) (I)	Description du produit de la solution de logiciels-services (J)	Information sur la Solution de logiciels-services (K)	Mots clés/étiquettes (L)
	(inscrire le numéro de pièce que l'éditeur de la Solution de logiciels-services utilise pour identifier la solution)	(inscrire le nom que l'éditeur de la Solution de logiciels-services utilise pour identifier la solution)	(inscrire le nom de l'éditeur de la Solution de logiciels-services qui produit la solution)	(inscrire le nom du fournisseur de services infonuagiques qui héberge la Solution de logiciels-services)	(inscrire le prix unitaire plafonds de la Solution de logiciels-services en dollars canadiens)	(inscrire le prix plafond pour les services professionnels (taux quotidiens, horaires ou forfaitaires) en dollars canadiens pour chaque catégorie : Guide de démarrage rapide (« GDR »), formation et services, services de mise en œuvre, services de formation, services d'épuration, de migration et de transition de données, et services consultatifs)	(inscrire l'unité de mesure pour la Solution de logiciels-services, par exemple « par utilisateur », « par entité », etc., **et** abonnement, durée)	(inscrire le pourcentage de remise qui sera appliqué aux prix unitaires commerciaux plafonds pour la durée de l'AMA)	(inscrire la langue de la Solution de logiciels-services (anglais et/ou français)	(entrez une brève description de la solution logiciels-services - le cas échéant)	(inscrire une adresse de site Web contenant de l'information sur la Solution de logiciels-services)	(inscrire des mots clés associés à la Solution de logiciels-services qui aideront les clients à chercher et trouver facilement les Solutions de logiciels-services qui répondent à leurs besoins)
1												
2												
3												

6.0 Partie 6 – Arrangement en matière d'approvisionnement est par les présentes supprimée dans son intégralité et remplacée par la version modifiables sous la section Pièces jointes de la page Avis d'appel d'offres: DAMA - Méthode d'approvisionnement de logiciels-services (Infonuagiques GC) (EN578-191593/F).

7.0 Section 7.2 et 7.3 du Partie 7 - Sélection des entrepreneurs et clauses de contrat subséquent est par les présentes supprimée et remplacée par le suivant :

7.2 Sélection de l'entrepreneur

(a) Besoins évalués à moins de 40 000 $ CAN (applicables taxes inclus)

(i) Source unique: Pour les besoins inférieurs à 40 000,00 $ CAN (applicables taxes inclus), le Canada peut choisir, à sa seule discrétion, de sous-traiter des contrats à un fournisseur ou de passer des contrats après la demande de soumissions.

(b) Besoins évalués à 40 000 $ CAN (TPS / TVH / TVQ incluse) ou plus

(i) Pour les besoins évalués à 40 000,00 $ CAN (applicables taxes inclus) ou plus, lorsqu'il n'y a qu'une seule source d'approvisionnement, le client doit fournir attestation de contrat à source unique et d'appel d'offres limitées conformément au les Règlement sur les marchés de l'État.

(ii) S'il n'existe qu'une seule source d'approvisionnement pour la solution de logiciel-service, le Canada peut demander au fournisseur de fournir un support de prix avant l'attribution du contrat. Le Canada se réserve le droit de négocier avec le fournisseur s'il est déterminé que les prix proposés ne représentent pas une bonne valeur pour le Canada.

(iii) Demande de soumissions: Pour les besoins évalués à 40 000,00 $ CAN (applicables taxes inclus) ou plus, si plusieurs solutions de logiciels-services disponibles dans le catalogue de logiciels-services peuvent répondre aux exigences techniques du Canada, le Canada émettre une demande de soumissions à tous les titulaires d'arrangement en matière d'approvisionnement qui offrent une solution qui répond aux exigences techniques du client en vertu de leur arrangement en matière d'approvisionnement. Si le Canada détermine que le catalogue de logiciels-services ne dispose pas de capacités suffisantes ou qu'il s'agit d'une exigence complexe et / ou spécialisée, il peut acquérir la solution de logiciels-services en dehors du catalogue de logiciels-services et étendre le concours à toutes les entreprises en publiant un document de demande de proposition officiel sur le SEAOG.

(c) Réservé/entreprise autochtone

(i) À la discrétion de chaque client, certaines sollicitations contre les AMA résultants peuvent être mises de côté pour des entreprises autochtones en vertu du CCSP du gouvernement fédéral.

(ii) Si le Canada souhaite passer un contrat en vertu du CCSP, il peut le faire en utilisant les AMA des fournisseurs autochtones. Toutes les conditions énoncées dans la présente AMA s'appliquent aux AMA des fournisseurs autochtones.

Veuillez également noter que le fractionnement des exigences (c.-à-d. La division d'un besoin en plusieurs exigences de moindre valeur monétaire) pour éviter un pouvoir d'approbation supérieur est contraire à la politique des marchés.

7.3 Procédures de demande de soumissions

(a) Des demandes de soumissions seront émises aux fournisseurs auxquels un arrangement en matière d'approvisionnement (AMA) a été émis, pour des besoins spécifiques dans le cadre de l'AMA.

(b) La demande de soumissions sera publiée par l'entremise du Service électronique d'appels d'offres du gouvernement SEAOG (www.achatetvente.gc.ca) et pourra être envoyée directement aux fournisseurs.

8.0 Annexe F - Clauses du contrat subséquent EN578-191593/F est par les présentes supprimée dans son intégralité et remplacée par la version modifiables sous la section Pièces jointes de la page Avis d'appel d'offres: DAMA - Méthode d'approvisionnement de logiciels-services (Infonuagiques GC) (EN578-191593/F).

9.0 Annexe H - Exigences relatives à la sécurité pour les entrepreneurs étrangers est par les présentes supprimée dans son intégralité et remplacée par le suivant :

ANNEXE H – Exigences relatives à la sécurité pour les entrepreneurs étrangers

Les clauses et conditions de sécurité étrangère suivantes s'appliquent à tout contrat résultant de la demande de soumissions et en font partie intégrante:

L'Autorité désignée en matière de sécurité pour le Canada (ADS canadien) est la Direction de la sécurité industrielle internationale (DSII), Secteur de la sécurité industrielle (SSI), Travaux publics et Services gouvernementaux Canada (TPSGC), administré par la Direction de la sécurité industrielle internationale (DSII), TPSGC. L'ADS canadien est chargée d'évaluer la conformité de **L'entrepreneur/Le sous-processeur/Le sous-traitant** aux exigences en matière de sécurité pour les fournisseurs étrangers. Les exigences de sécurité suivantes s'appliquent à l'entrepreneur étranger destinataire constituée ou autorisé à faire des affaires dans une administration autre que le Canada et la prestation ou l'exécution à l'extérieur du Canada les services et/ou travaux décrits dans les solutions cloud, en plus des exigences en matière de sécurité et de protection, détaillé dans les annexes C et D, respectivement. Ces exigences en matière de sécurité sont en plus des exigences énoncées dans la section intitulée Protection et sécurité des données stockées dans des bases de données.

1. **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit être dans un pays de l'Union européenne, dans un pays de l'organisation du traité de l'Atlantique Nord (OTAN) ou dans un des pays avec lesquels le Canada a conclu une entente en matière de sécurité et un protocole d'entente bilatérale ou multinationale. Le programme de sécurité a des ententes en matière de sécurité et protocole d'entente bilatérale ou multinationale avec les pays mentionnés au site de TPSGC suivant: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html.

2. **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit en tout temps, au cours de la durée du **contrat/sous-traitance**, être inscrits auprès de l'autorité nationale de supervision de la protection des renseignements personnels appropriée des pays dans lesquels ils sont incorporés ou autorisé à exercer des activités commerciales. **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit fournir une preuve de son enregistrement avec l'autorité de supervision applicables à l'autorité contractante et l'autorité contractante en matière de sécurité et de cerner les renseignements personnels pertinents à l'échelle nationale. Pour **L'entrepreneur/Le sous-processeur/Le sous-traitant** européens, ce sera l'autorité de protection des données nationales (APDN).

3. **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit, en tout temps durant l'exécution du **contrat/sous-traitance**, tenir une équivalence à une vérification d'organisation désignée (VOD), délivrée par l'ADS canadien comme suit :

    i. **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit fournir une preuve qu'il est incorporé ou autorisé à faire affaire dans son champ de compétence.

    ii. **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire ne doit pas entreprendre les travaux, fournir les services ou assurer toute autre prestation tant que l'Administration désignée en matière de sécurité au Canada (ADS canadien) n'a pas confirmé le respect de toutes les conditions et exigences en matière de sécurité stipulées dans le **contrat/sous-traitance**. L'ADS canadien donne cette confirmation par écrit **à l'entrepreneur/au sous-processeur/au sous-traitant** étranger destinataire. Un Formulaire d'attestation remis par l'ADS canadien **à l'entrepreneur/au sous-processeur/au sous-traitant** étranger destinataire permettra de confirmer la conformité et l'autorisation de fournir les services prévus.

    iii. **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire proposé doit identifier l'agent de sécurité du contrat (ASC) autorisé et un agent remplaçant de sécurité d'entreprise (ARSE) (le cas échéant) qui sera responsable du contrôle des exigences de sécurité, telles qu'elles sont définies dans le **contrat/sous-traitance**. Cette personne sera désignée par le président-directeur général ou par un cadre supérieur clé de l'entreprise étrangère destinataire proposée. Les cadres supérieurs clés comprennent les propriétaires, les agents, les directeurs, les cadres et les partenaires occupant un poste qui leur permettrait d'avoir une influence sur les politiques ou les pratiques de l'organisation durant l'exécution du **contrat/sous-traitance**.

iv. **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire n'autorisera pas l'accès à des renseignements/biens de niveau **CANADA PROTÉGÉ**, sauf aux membres du personnel qui ont fait l'objet d'une vérification de sécurité conformément à la définition et aux pratiques énoncées dans la Norme sur le filtrage de sécurité (https://www.tbs-sct.gc.ca/pol/docfra.aspx?id=28115) du Conseil du Trésor, ou qui utilisent des mesures équivalentes acceptables établies par l'entrepreneur dans ses documents publics, et comme convenu par l'ADS canadienne, notamment, sans toutefois s'y limiter**:**

a. Le personnel a un besoin de savoir pour l'exécution du **contrat/sous-traitance**;

b. Le personnel a fait l'objet d'une vérification du casier judiciaire valide, avec des résultats favorables, d'une agence gouvernementale reconnue ou d'une organisation du secteur privé dans **leur pays**, ainsi qu'une vérification d'antécédents, validé par l'ADS canadien.

c. **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit s'assurer que le personnel consente à la divulgation du casier judiciaire et antécédents à l'ADS canadien et d'autres fonctionnaires du gouvernement canadien, si demandé; et

d. Le Gouvernement du Canada se réserve le droit de refuser l'accès aux renseignements/ biens de niveau **CANADA PROTÉGÉ à l'entrepreneur/au sous-processeur/au sous-traitant** étranger destinataire pour cause.

4. Les renseignements/biens de niveau **CANADA PROTÉGÉ** fournis ou produits dans le cadre **du contrat/sous-traitance** ne doivent pas être remis à un autre sous-traitant étranger destinataire, sauf dans les cas suivants:

a. L'ADS canadien atteste par écrit que le sous-traitant étranger destinataire a obtenu l'accès aux renseignements/biens de niveau **CANADA PROTÉGÉ** par l'intermédiaire de l'ADS canadien;

b. L'ADS canadien donne son autorisation écrite lorsque l'autre sous-traitant étranger destinataire est situé dans un autre pays.

5. **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire NE DOIT PAS emporter de renseignements/ biens de niveau **CANADA PROTÉGÉ** hors des établissements de travail visés, et **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit s'assurer que son personnel est au courant de cette restriction et qu'il la respecte.

6. **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire ne doit pas utiliser les renseignements/biens de niveau **CANADA PROTÉGÉ** pour répondre à des besoins distincts de l'exécution du **contrat/sous-traitance** sans l'approbation écrite préalable du gouvernement du Canada. Cette autorisation doit être obtenue auprès de auprès de l'ADS canadien.

7. **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit, en tout temps durant l'exécution du **contrat/sous-traitance** tenir une équivalence à une autorisation de détenir des renseignements (ADR) de **CANADA PROTÉGÉ A ou B**, selon le cas.

Tous les renseignements/biens de niveau **CANADA PROTÉGÉ** fournis **à l'entrepreneur/au sous-processeur/au sous-traitant** étranger destinataire ou produits par ce dernier doivent être aussi protégés comme suit:

8. **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit signaler immédiatement à l'ADS canadien tous les cas dans lesquels il est connu où il a lieu de soupçonner que les renseignements/biens de niveau **CANADA PROTÉGÉ** obtenus dans le cadre du **contrat/sous-traitance** ont été compromis.

OU

9. **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit signaler immédiatement à l'ADS canadien tous les cas dans lesquels il sait où il a lieu de croire que des renseignements/biens de niveau **CANADA PROTÉGÉ** fournis ou produits par **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire conformément au **contrat/sous-traitance** ont été perdus ou divulgués à des personnes non autorisées.

10. **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire ne doit pas divulguer les renseignements/biens de niveau **CANADA PROTÉGÉ** à un tiers, qu'il s'agisse d'un gouvernement, d'un particulier, d'une entreprise ou de ses représentants, sans l'accord écrit préalable du gouvernement du Canada. Cet accord doit être obtenu par l'ADS canadien.

11. **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire assurera une protection des renseignements/biens de niveau **CANADA PROTÉGÉ** aussi stricte que celle mise en œuvre par le gouvernement du Canada, conformément aux politiques, aux lois et aux règlements nationaux en matière de sécurité nationale, et comme prévu par l'ADS canadien.

12. À la fin des services et/ou travaux, **L’entrepreneur/Le sous-processeur/Le sous-traitant** destinataire doit restituer au gouvernement du Canada tous les renseignements/biens de niveau **CANADA PROTÉGÉ** qu'il aura reçus ou produits en vertu du **contrat/sous-traitance**, y compris tous les renseignements/biens de niveau **CANADA PROTÉGÉ** remis à ses sous-traitants ou produits par eux.

13. **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire exigeant aux renseignements/biens de niveau **CANADA PROTÉGÉ** ou aux sites à accès restreint en vertu **du contrat/sous-traitance**, doit présenter une demande pour l’accès au site à l’agent de sécurité ministériel du ministère de Département / Organisation pour lequel les Services et / ou Travaux sont exécutés dans le cadre du Contrat**.**

14. **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire NE DOIT PAS utiliser ses systèmes de technologie de l'information pour traiter, produire ou stocker dans un système informatique des renseignements de niveau **CANADA PROTÉGÉ B** avant que l'ADS canadien lui en donne le droit.

15. **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doivent s’assurer que toutes les bases de données y compris les bases de données de sauvegarde utilisées par les organisations pour offrir les services décrits à l’énonce de travaux contenant des renseignements de niveau **CANADA PROTÉGÉ B** liés aux services et/ou travaux se trouvent dans le Canada.

16. Les sous-traitances comportant des exigences relatives à la sécurité NE doivent PAS être attribuées sans l'autorisation écrite préalable de l'ADS canadien.

17. Tous les contrats de sous-traitance attribués à un entrepreneur étranger destinataire ne doivent PAS être attribués sans l’autorisation écrite préalable de l’AVD canadienne afin de confirmer les exigences de sécurité à imposer aux sous-traitants.

18. Tous les contrats de sous-traitance attribués par un entrepreneur étranger destinataire ne doivent PAS être attribués sans l’autorisation écrite préalable de l’AVD canadienne afin de confirmer les exigences de sécurité à imposer aux sous-traitants.

19. **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit se conformer aux dispositions de la Liste de vérification des exigences relatives à la sécurité figurant à l'Annexe I.

20. Le Canada a le droit de rejeter toute demande présentée de manière distincte et indépendante de l’autorisation contenue dans le présent contrat relativement à l’autorisation de l’entrepreneur qui fournit les services d’accéder, de traiter, de produire, de transmettre ou de stocker électroniquement des renseignements ou des actifs **CANADA PROTÉGÉ** liés aux prestation de services et/ou travaux dans un autre pays s'il y a des raisons de croire que leur sécurité, leur confidentialité ou leur intégrité pourrait être menacée.

Protection et sécurité des données stockées dans des bases de données

1. **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit s'assurer que toutes les bases de données utilisés par les organisations pour fournir les services décrits dans les solutions cloud contenant des renseignements **CANADA PROTÉGÉ B**, liées au services et/ou travail, se trouvent au Canada.

2. **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit contrôler l'accès à toutes les bases de données dans lesquelles sont stockées des données liées au **contrat/sous-traitance**, afin que seules les personnes qui ont la cote de sécurité appropriée puissent avoir accès à la base de données, soit au moyen d'un mot de passe ou d'un autre moyen d'accès (comme des mesures de contrôle biométrique).

3. **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit s'assurer que toutes les bases de données contenant des données relatives au contrat / sous-contrat sont physiquement et logiquement indépendantes (ce qui signifie qu'il n'y a pas de connexion directe ou indirecte) avec toutes les autres bases de données.

4. **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit s'assurer que toutes les données liées au **contrat/sous-traitance** sont traitées uniquement au Canada ou dans un autre pays approuvé par l’autorité contractante conformément au paragraphe 1.

5. **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit s'assurer que le trafic sur le réseau national (c'est-à-dire le trafic partant d'une partie du Canada vers une destination située dans une autre partie du Canada) s'effectue exclusivement au Canada, sauf si l'autorité contractante a approuvé au préalable, par écrit, une autre route. L’autorité contractante prendra uniquement en considération une route dans un autre pays pour la transmission de données, si ce pays respecte les exigences décrites au paragraphe 1.

6. Malgré tout article des conditions générales relatif à la sous-traitance, **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire ne peut confier à un sous-traitant (y compris à une société affiliée) aucune fonction qui permet d'accéder aux données du **contrat/sous-traitance** sans le consentement écrit préalable de l'autorité contractante.

Renseignements personnels

Interprétation

Dans le **contrat/sous-traitance**, à moins que le contexte n'indique un sens différent,

« Conditions générales » désigne les conditions générales qui font partie du **contrat/sous-traitance** ;

« Renseignement personnel » désigne tout renseignement qui concerne un individu, y compris le type de renseignements décrit à la section 3 de la *Loi sur la protection des renseignements personnel*s, L.R.C. 1985, ch. P-21.

« Dossier » désigne un exemplaire papier ou des données sous forme lisible par machine comprenant des renseignements personnels.

Les mots et expressions définis dans les conditions générales et utilisés dans le présent article ont le sens qui leur est donné dans les conditions générales.

Propriété des renseignements personnels et des dossiers

Pour exécuter les services et/ou travaux, **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire aura accès à des renseignements personnels de tiers et(ou) en recueillera. **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire reconnaît qu'il ne détient aucun droit sur ces renseignements personnels ou ces dossiers. **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit rendre disponibles, sur demande du Canada, tous les renseignements personnels et dossiers dans un format acceptable pour le Canada.

Utilisation des renseignements personnels

L’entrepreneur/Le sous-processeur/Le sous-traitant étranger destinataire convient de créer, de recueillir, de recevoir, de gérer, de consulter, d’utiliser, de conserver, de divulguer et de disposer des renseignements personnels et des dossiers uniquement pour exécuter les services et/ou travaux conformément au contrat, et ce, conformément aux dispositions du présent **contrat/sous-traitance**.

Cueillette des renseignements personnels

1. Si **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit obtenir des renseignements personnels d'un tiers dans le cadre des services et/ou travaux, il ne doit recueillir que les renseignements personnels lui permettant d'exécuter les services et/ou travaux. **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit recueillir les renseignements personnels auprès de l’individu concerné et l’informer (au moment de la cueillette ou préalablement) de ce qui suit :

   a) les renseignements personnels sont recueillis au nom du Canada et lui seront transmis;

   b) les usages qui seront faits des renseignements personnels recueillis;

   c) que la divulgation des renseignements personnels est volontaire ou, s'il existe une obligation juridique de divulguer les renseignements personnels, les fondements de cette obligation juridique;

d) les conséquences, s'il en est, du refus de fournir les renseignements;

e) que l'intéressé au droit d'accéder à ses renseignements personnels et d'y apporter des corrections;

f) les renseignements personnels feront partie d'un fichier de renseignements personnels particulier (au sens de la *Loi sur la protection des renseignements personnels*), et fournir à l'individu de l'information concernant l'institution fédérale qui gère le fichier de renseignements personnels, si l'autorité contractante a fourni ces renseignements **à l'entrepreneur/au sous-processeur/au sous-traitant** étranger destinataire.

2. **L'entrepreneur/Le sous-processeur/Le sous-traitant** et leurs employés respectifs doivent s'identifier auprès des individus desquels ils recueillent des renseignements personnels et leur donner le moyen de vérifier qu'ils sont autorisés à recueillir les renseignements personnels en vertu d'un contrat passé avec le Canada.

3. Si l'autorité contractante l'exige, **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit élaborer un formulaire de demande de consentement à utiliser lors de la cueillette de renseignements personnels ou un texte dans le cas de la cueillette de renseignements personnels par téléphone. **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire ne peut utiliser le formulaire ou le texte sans avoir obtenu l'approbation écrite préalable de l'autorité contractante. Il doit aussi obtenir le consentement de l'autorité contractante avant de modifier le formulaire ou le texte.

4. Si, lors de la cueillette de renseignements personnels auprès d'un individu, **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire sait ou soupçonne que cet individu n'est pas en mesure de consentir à la divulgation et à l'utilisation de ses renseignements personnels, **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit demander des directives à l'autorité contractante.

Exactitude, confidentialité et intégrité des renseignements personnels

L'entrepreneur/Le sous-processeur/Le sous-traitant étranger destinataire doit veiller à ce que les renseignements personnels soient les plus exacts, complets et à jour que possible. Pour ce faire, **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit, au minimum:

a) ne pas utiliser de données d'identification personnelle (par ex., le numéro d'assurance sociale, le numéro de passeport, le numéro d'identificateur client unique) pour lier de nombreuses bases de données qui comprennent des renseignements personnels;

b) isoler les dossiers des renseignements et des dossiers de **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire**;**

c) ne donner l'accès aux renseignements personnels et aux dossiers qu'à ceux qui le requièrent aux fins d'exécution des services et/ou travaux (par exemple, en utilisant des mots de passe ou un accès biométrique);

d) donner de la formation à toute personne à laquelle **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire donne accès aux renseignements personnels concernant l'obligation d'assurer la confidentialité et de ne l'utiliser qu'aux fins d'exécution des services et/ou travaux. **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit donner cette formation avant d'autoriser l'accès aux renseignements personnels et préparer à cet effet un dossier accessible à l'autorité contractante, sur demande;

e) à la demande de l'autorité contractante, demander aux personnes ayant accès aux renseignements personnels de reconnaître, par écrit (sous une forme approuvée par l'autorité contractante), leurs responsabilités en matière de confidentialité des renseignements personnels, avant de leur en donner l'accès;

f) tenir un registre de toutes les demandes faites par un individu pour la révision de ses renseignements personnels et toutes les demandes de correction d'erreurs ou d'omissions concernant les renseignements personnels (que les demandes soient faites directement par un individu ou par le Canada au nom d'un individu);

g) joindre une note à tout dossier qu'un individu a demandé de corriger, mais que **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire a décidé, pour quelque raison que ce soit,

de ne pas corriger. Lorsque cela se produit, l'entrepreneur doit immédiatement informer l'autorité contractante de la correction demandée et des raisons de **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire de ne pas l'effectuer. Si l'autorité contractante demande que la correction soit effectuée, **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire a l'obligation de le faire;

h) tenir un registre de la date et de l'auteur de la dernière mise à jour de chaque dossier;

i) maintenir un journal de vérification électronique qui enregistre tous les accès et les tentatives d'accès des dossiers électroniques. Le journal de vérification doit être dans un format qui peut être lu par **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire et le Canada en tout temps;

j) sécuriser et contrôler l'accès à tout renseignement personnel.

Protection des renseignements personnels

L'entrepreneur/Le sous-processeur/Le sous-traitant étranger destinataire doit protéger les renseignements personnels à tout moment en prenant toutes les mesures raisonnablement nécessaires pour les protéger et en protéger l'intégrité et la confidentialité. Pour ce faire, **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit au moins:

a) stocker les renseignements personnels sous format électronique de manière à ce qu'un mot de passe (ou un autre mécanisme de contrôle) soit requis pour accéder au système ou à la base de données où sont stockés les renseignements personnels;

b) s'assurer que les mots de passe ou autres moyens d'accès aux renseignements personnels ne sont fournis qu'aux individus qui le requièrent aux fins d'exécution des services et/ou travaux;

c) ne pas confier à un tiers (y compris un affilié) le stockage des renseignements personnels sans l'autorisation préalable et écrite de l'autorité contractante;

d) protéger les bases de données ou les systèmes informatiques qui emmagasinent les renseignements personnels contre un accès externe de manière à protéger les renseignements très protégés et de nature délicate;

e) faire une sauvegarde et une mise à jour de tous les dossiers au moins une fois par semaine;

f) mettre en œuvre toutes les mesures de sécurité ou de protection demandées par le Canada de temps à autre;

g) aviser immédiatement l'autorité contractante de toute infraction (p. ex. un accès, un usage ou une divulgation non autorisé de renseignements) ou de tout incident pouvant mettre en danger la sécurité ou l'intégrité des dossiers, des systèmes ou des installations ou des renseignements personnels sont conservés. Si une infraction se produit, l'entrepreneur ou le sous-traitant devra immédiatement prendre toutes les mesures raisonnables nécessaires pour limiter l'étendue des impacts possibles ou pour résoudre le problème et empêcher celui-ci de se reproduire. Le Canada peut exiger de l'entrepreneur qu'il prenne des mesures précises pour régler le problème et éviter qu'il se reproduise, et pourrait invoquer les dispositions de la présente entente en lien avec la suspension ou la résiliation du contrat pour manquement.

Obligation de présenter des rapports trimestriels

Dans un délai de trente (30) jours suivant la fin de chaque trimestre (janvier-mars; avril-juin; juillet-septembre; octobre-décembre), **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit présenter à l'autorité contractante:

a) une description de toute nouvelle mesure qu'il a prise pour protéger les renseignements personnels (par exemple, un nouveau logiciel ou de nouveaux contrôles d'accès utilisés par **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire);

b) une liste des corrections apportées aux renseignements personnels à la demande d'un individu (y compris le nom de la personne, la date de la demande et la correction apportée);

c) les détails de toute plainte reçue d'individus concernant la manière dont leurs renseignements personnels sont recueillis ou traités par **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire;

d) une copie (dans un format électronique convenu par l'autorité contractante et **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire) de l'ensemble des renseignements personnels conservés électroniquement par **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire.

Évaluation des menaces et des risques

L'entrepreneur/Le sous-processeur/Le sous-traitant étranger destinataire doit présenter à l'autorité contractante une évaluation des menaces et des risques dans un délai de quatre-vingt-dix (90) jours suivant l'attribution du **contrat/sous-traitance**, et dans un délai de trente (30) jours civils suivant chaque date d'anniversaire du contrat s'il dure plus d'un an, qui doit comprendre:

a) une copie de la dernière version du formulaire de demande de consentement ou du script que **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire utilise pour recueillir les renseignements personnels;

b) une liste des types de renseignements personnels utilisés par **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire se rapportant aux services et/ou travaux;

c) une liste de tous les emplacements où les exemplaires papiers des renseignements personnels sont conservés;

d) une liste de tous les emplacements où les renseignements personnels sous forme lisible par machine sont conservés (par exemple, l'emplacement du serveur sur lequel la base de données est installée), ainsi que les sauvegardes;

e) une liste de toutes les personnes auxquelles **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire a donné l'accès aux renseignements personnels ou aux dossiers;

f) une liste de toutes les mesures prises par **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire pour protéger les renseignements personnels et les dossiers;

g) une explication détaillée des menaces réelles ou potentielles touchant les renseignements personnels ou les dossiers, accompagnée d'une évaluation des risques créés par ces menaces et la pertinence des protections existantes visant à prévenir ces risques; et

h) une explication de toute nouvelle mesure que **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire considère prendre afin de protéger les renseignements personnels et les dossiers.

Vérification et conformité

Le Canada peut vérifier en tout temps la conformité de **l'entrepreneur/le sous-processeur/le sous-traitant** étranger destinataire aux articles relatifs à la protection des renseignements personnels. À la demande de l'autorité contractante, **l'entrepreneur/le sous-processeur/le sous-traitant** étranger destinataire doit donner au Canada (ou à son représentant autorisé) l'accès à ses locaux et aux renseignements personnels et dossiers en tout temps jugé raisonnable. Si le Canada découvre un problème durant la vérification, **l'entrepreneur/le sous-processeur/le sous-traitant** étranger destinataire doit le corriger immédiatement à ses frais.

Obligations réglementaires

1. **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire reconnaît que le Canada est tenu de traiter tous les renseignements personnels et les dossiers conformément aux dispositions de la **Loi sur la protection des renseignements personnels**, de la **Loi sur l'accès à l'information**, L.R.C.1985, ch. A-1, et de la **Loi sur la Bibliothèque et les Archives du Canada**, L.C. 2004, ch.11. **L'entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire convient de se conformer aux exigences établies par l'autorité contractante qui sont requises pour permettre au Canada de remplir ses obligations en vertu de ces lois et toute autre loi qui entre en vigueur lorsqu'il y a lieu.

2. **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire reconnaît que les obligations dont il doit s'acquitter en vertu du contrat s'ajoutent à toutes celles qui lui incombent en vertu de la **Loi sur la protection des renseignements personnels et les documents électroniques**, L. C. 2000, ch.5, ou d'une loi similaire en vigueur dans une province ou un territoire du Canada. Si **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire estime que l’une ou l’autre des obligations du contrat l’empêche de s’acquitter de ses obligations en vertu de ces lois, il doit immédiatement informer l’autorité contractante de la disposition du contrat et de l’obligation de la loi qu’il considère comme contradictoires.

Élimination et retour des dossiers au Canada

L’entrepreneur/Le sous-processeur/Le sous-traitant étranger destinataire ne peut éliminer aucun dossier à moins que l’autorité contractante le lui demande. Sur demande de l'autorité contractante, ou lorsque les services et/ou travaux liés aux renseignements personnels sont achevés, le contrat est achevé ou lorsque le contrat est résilié, selon ce qui se produit en premier, **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit retourner tous les dossiers (y compris les copies) à l'autorité contractante.

Obligation juridique de divulguer les renseignements personnels

Avant de divulguer tout renseignement personnel conformément à toute loi, à tout règlement ou toute ordonnance rendue par une cour de justice, un tribunal ou une entité administrative compétente, **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit immédiatement informer l’autorité contractante afin de lui permettre de participer aux procédures pertinentes.

Plaintes ou demandes d'accès

Le Canada et **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire conviennent de s’informer immédiatement et mutuellement de la réception d’une plainte en vertu de la *Loi sur l’accès à l’information*, de la *Loi sur la protection des renseignements personnels* ou de toute autre loi pertinente concernant les renseignements personnels. Les parties conviennent de s’échanger toute information nécessaire pour faciliter le règlement de la plainte et de s’informer immédiatement et mutuellement de son dénouement.

Exception

Les obligations énoncées dans ces articles ne s'appliquent pas aux renseignements personnels qui sont déjà du domaine public, du moment qu'elles ne sont pas devenues du domaine public, à la suite d'une faute ou d'une omission de l'entrepreneur/le sous-traitant étranger destinataire ou de tout sous-traitant, agent ou représentant de l'entrepreneur ou de leurs employés.

SECRET

Une autorisation secret sera requise pour tous les personnels de L’entrepreneur/Le sous-processeur/Le sous-traitant qui a des privilèges élevés assortis d’un accès logique sans restriction aux données du GC hébergées dans les centres de données de l’entrepreneur, à tout système sensible, de même qu’aux données sur les incidents de sécurité.

L’entrepreneur et les sous-traitants doivent être dans un des pays avec lesquels le Canada a conclu une entente en matière de sécurité industrielle et un protocole d’entente bilatéral ou multinational, ou qui possèderont un tel instrument avec le Canada avant la fin de la période de soumission. Le programme de sécurité des contrats (PSC) à des ententes en matière de sécurité industrielle, protocole d’entente bilatéral ou multinational industrielle avec les pays mentionnés au site suivant de SPAC: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html.

1. Les contrats de sous-traitance comportant des exigences relatives à la sécurité NE doivent PAS être attribués sans l'autorisation écrite préalable de l’Autorité nationale de la sécurité (ANS) ou l’Autorité désignée en matière de sécurité (ADS) concernée, conformément aux législations, règlements, et politiques nationales du pays du fournisseur / ADS canadienne.
2. **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire NE DOIT PAS utiliser ses systèmes de technologie de l'information pour traiter, produire ou conserver dans un système informatique et transférer au moyen d'un lien électronique des renseignements/biens de niveau **CANADA PROTÉGÉ / CLASSIFIÉ** avant que l’Autorité nationale de la sécurité (ANS) ou l’Autorité désignée en matière de sécurité (ADS) **du pays du fournisseurs** lui en donne le droit.

Une fois que **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire a reçu cette approbation écrite, il peut effectuer ces tâches jusqu’au niveau **SECRET**.

3. **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire ne doit pas utiliser les renseignements /biens de niveau **CANADA PROTÉGÉ/CLASSIFIÉ** pour répondre à des besoins distincts de l'exécution **du contrat/de l'offre à commandes/du contrat de sous-traitance** sans l'approbation écrite préalable du gouvernement du Canada. Cette autorisation doit être obtenue auprès de l'ADS du Canada.
4. **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit signaler immédiatement à l'ADS canadienne tous les cas pour lesquels il sait où il a lieu de croire que des renseignements/biens de niveau **CANADA PROTÉGÉ / CLASSIFIÉ** obtenus dans le cadre **du présent contrat / de la présente offre à commandes / du présent contrat de sous-traitance** ont été compromis.
5. **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire ne doit pas divulguer les renseignements/biens de niveau **CANADA PROTÉGÉ/CLASSIFIÉ** à un tiers, qu'il s'agisse d'un gouvernement, d'un particulier, d'une entreprise ou de ses représentants, sans l'accord écrit préalable du gouvernement du Canada. Cet accord doit être obtenu par l'intermédiaire de l’Autorité nationale de la sécurité (ANS) ou de l’Autorité désignée en matière de sécurité (ADS) du destinataire / ADS du Canada.
6. **L’entrepreneur/Le sous-processeur/Le sous-traitant** étranger destinataire doit se conformer aux dispositions de la Liste de vérification des exigences relatives à la sécurité figurant à l'Annexe I.

10.0 Présentation de la journée de l’industrie sur la DAMA logiciels-services de niveau Protégé :

Serving GOVERNMENT, serving CANADIANS. Au service du GOUVERNEMENT, au service des CANADIENS.

Demande d'arrangement en matière d'approvisionnement (DAMA) pour des logiciels-services infonuagiques SaaS Protégés

Bienvenue à la journée de l'industrie

11 Janvier 2021

9:00 am a 12:00 pm

Direction de l'approvisionnement en logiciels
Services publics et Approvisionnement Canada

Nº de la DAMA sur Achatsetventes.gc.ca : EN578-191593/F

Mot de bienvenue et introduction

Nº de la DAMA sur Achatsetventes.gc.ca : EN578-191593/F

DAMA Saas Protégés - Journée de l’industrie

Ordre du jour

Durée	Description et objectifs
De 9 h 00 à 09 h 05	Mot de bienvenue et présentations – SPAC
De 9 h 05 à 9 h 15	Objectifs de la journée de l’industrie – SPAC
De 9 h 15 à 9 h 45	Présentation de l’outil d’approvisionnement – SPAC
De 9 h 45 à 10 h 30	Exigences relatives à la sécurité – SPAC, CCCS et CST
De 10 h 30 à 11 h 00	Exigences financières – SPAC
De 11 h 00 à 11 h 40	Questions et réponses – Industrie
De 11 h 40 à 11 h 45	Mot de la fin – SPAC

DAMA SaaS Protégés - Journée de l'industrie

L'exposé vise à fournir aux fournisseurs des renseignements et de l'orientation sur la manière de participer dans le cadre du présent outil d'approvisionnement pour répondre aux exigences et aux besoins opérationnels.

Exposé sur l’outil d’approvisionnement de SaaS Protégés

Table des matières

DAMA SaaS - Avantages pour l'industrie

- Augmentation des opportunités des ventes avec le GC (liste de distribution interne et publication enligne)

- Processus de qualification facilité et nouvelle approche collaborative avec SPAC
- Approche flexible afin de mettre a jour la liste de produits et de prix (plus de fiches ou de tableurs)
- Méthode d'arrangement en matière d'approvisionnement (DAMA) pour la vente des logiciels-services infonuagiques protégés B
- Nouvelle limitation de responsabilité juste et raisonnable adaptée aux logiciels-services infonuagiques
- Soutien du GC vers les nouveaux objectifs de transformation numérique

Nº de la DAMA sur Achatsetventes.gc.ca : EN578-191593/F

1. Transformation numérique (1/2)

Facteur opérationnel 1 : Appuyer la Stratégie d'adoption de l'informatique en nuage du GC

L'industrie du logiciel évolue rapidement vers un écosystème axé sur l'informatique en nuage. Ainsi, le GC adopte une mesure proactive pour répondre à cette évolution.

« C'est pourquoi la Stratégie d'adoption de l'informatique en nuage exige que les DPI considèrent d'abord le modèle de prestation de services d'informatique en nuage publics et le modèle de logiciel en tant que service (SaaS), car ces modèles sont ceux qui offrent les plus grands avantages au GC ».*

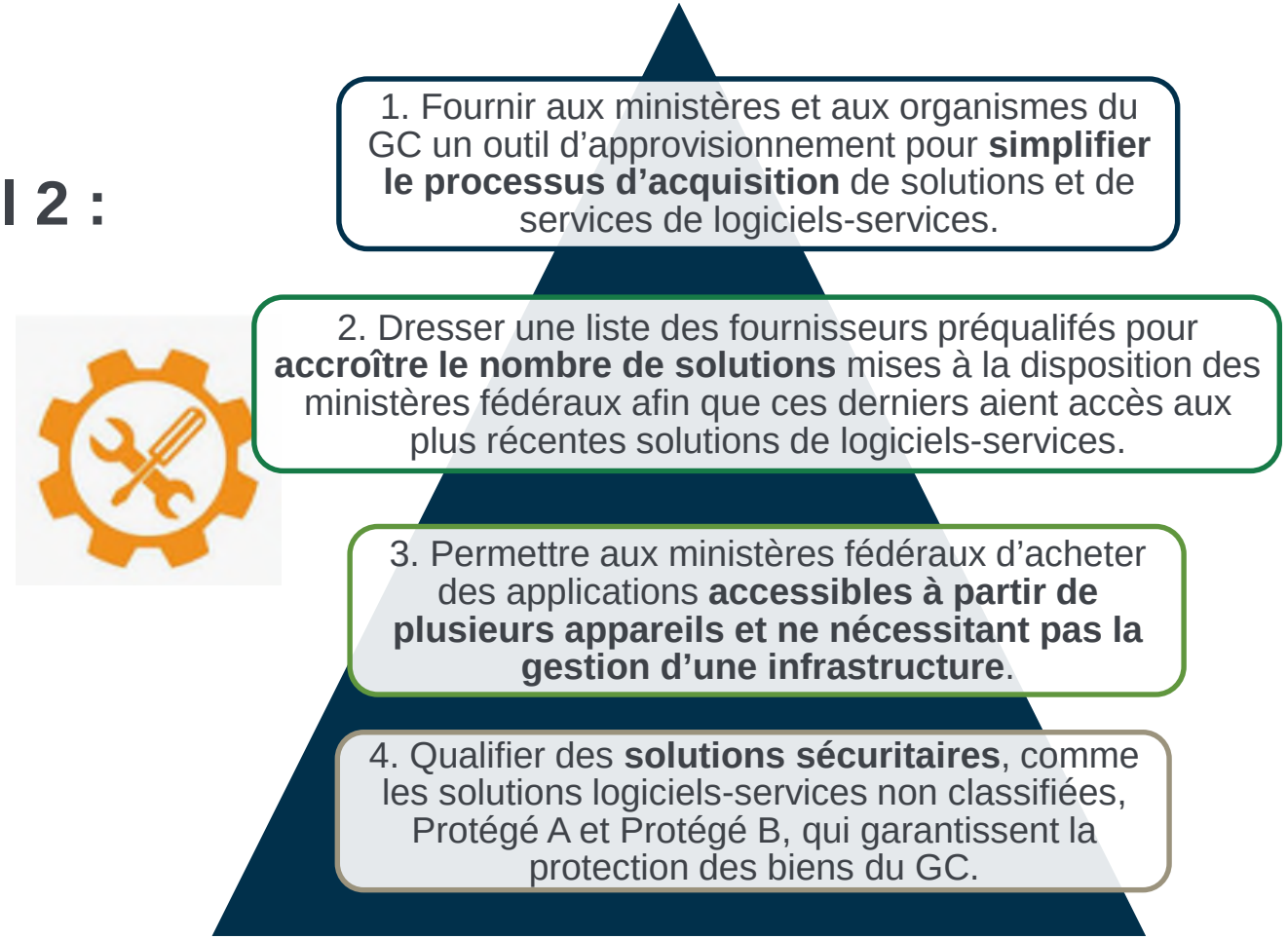
La stratégie d'adoption de « l'**informatique en nuage d'abord** » privilégie l'infonuagique pour la prestation des services de TI, ainsi que le nuage public pour le déploiement infonuagique au sein des ministères.

*Stratégie d'adoption de l'informatique en nuage du GC : Mise à jour de 2018

Nº de la DAMA sur Achatsetventes.gc.ca : EN578-191593/F

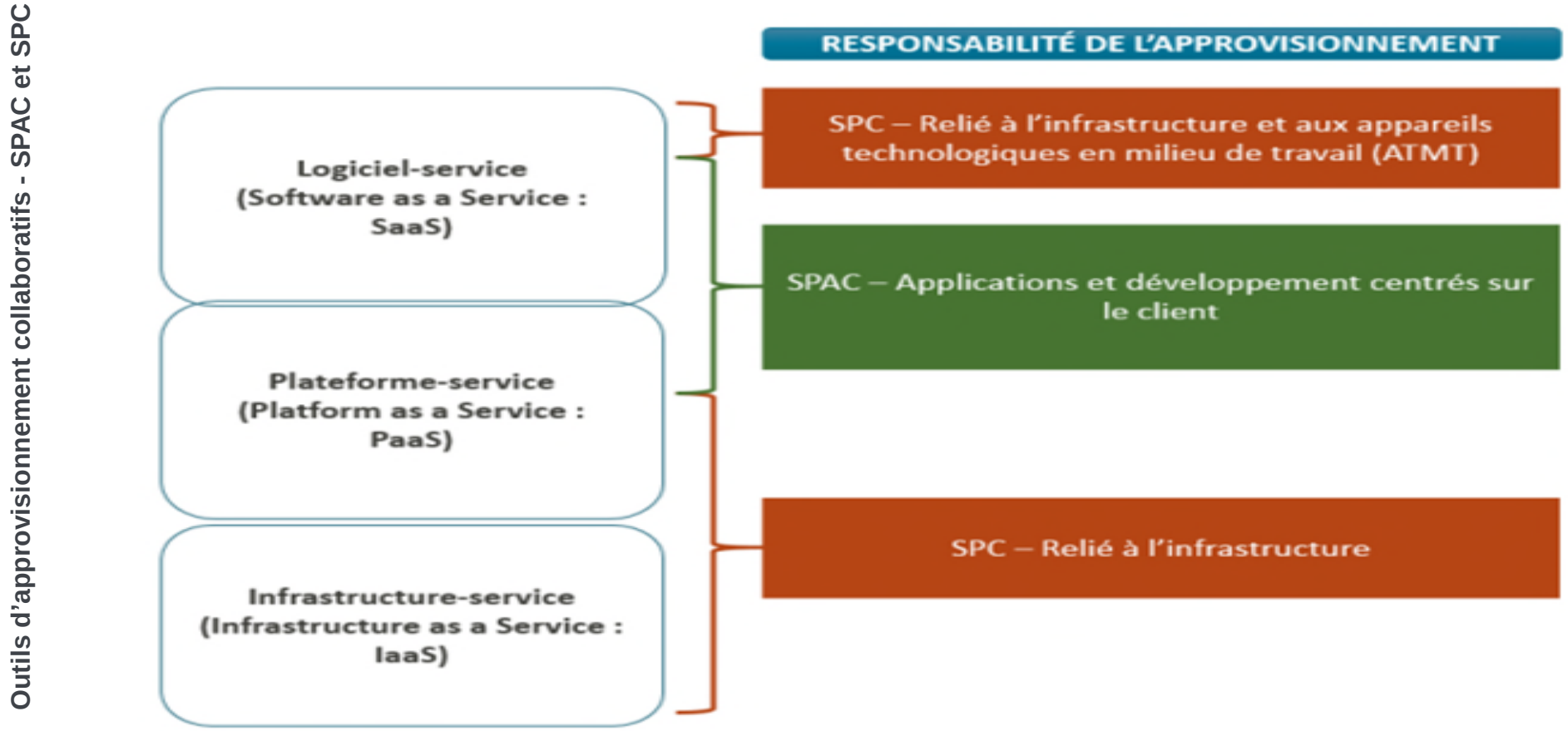
1. Transformation numérique (2/2)

Facteur opérationnel 2 : Buts et objectifs



Nº de la DAMA sur Achatsetventes.gc.ca : EN578-191593/F

2. Rôles et responsabilités en matière d'approvisionnement relatif à l'infonuagique du GC



Nº de la DAMA sur Achatsetventes.gc.ca : EN578-191593/F

3. Processus de la DAMA SaaS GC

Innovation

- Une demande de renseignements a été diffusée pour harmoniser nos exigences aux normes de l'industrie.
- Plus de 40 séances individuelles ont été organisées pour obtenir des commentaires
- Intégration de la rétroaction de l'industrie
- Simplification des modalités contractuelles.
- Nouvelles clauses de responsabilitées

Processus évolutif

- La Dama est un processus continu, qui n'a pas de date de clôture ferme.
- Le processus collaboratif de qualification offre une certaine souplesse aux fournisseurs pour se qualifier.
- Permet aux ministères clients de se procurer des solutions de logiciels-services de façon continue.

Sécurité

- Sélection et respect des normes de sécurité infonuagique du GC,
- Tire profit des normes de sécurité industrielle disponibles sur le marché

Collaboration

- Tirer profit d'une approche de processus d'approvisionnement collaborative pour faciliter le processus de soumission.
- Approche multi ministérielle contractuelle

Nº de la DAMA sur Achatsetventes.gc.ca : EN578-191593/F

4. Aperçu de l’AMA SaaS Protégés

La première phase consiste à qualifier les fournisseurs par le biais de la DAMA affichée en permanence sur l'Achat et la Vente. Les fournisseurs qualifiés se verront accorder un arrangement en matière d'approvisionnement.

La deuxième phase consiste à attribuer des contrats aux titulaires d'arrangements en matière d'approvisionnement via une demande de soumissions simplifiées ou en émettant des contrats à fournisseur unique lorsque toutes les justifications obligatoires sont remplies.

5. Critères dévaluation normalisés (1/5)

La DAMA applique divers critères normalisés pour évaluer la capacité des fournisseurs à satisfaire aux besoins du Canada, y compris :

Critères techniques

- Exigences de qualification
- Obligations relatives à la sécurité et à la protection des renseignements personnels
- Entente sur les niveaux de service du fournisseur
- Présentation des formulaires

Critères financiers

- Tarifs indicatifs + taux de réduction applicable
- Unité de mesure (par exemple, « par utilisateur », « par utilisation », etc.)

Exigences relatives à la sécurité et aux certifications liées aux TI

- Certifications en sécurité industrielle (selon le tiers)
- Processus d'ICA et d'évaluation de la sécurité des TI

5. Critères d’évaluation normalisés (2/5)

Processus détaillé de présentation de la proposition financière

- ✓ Les fournisseurs doivent présenter l’annexe C, Catalogue de solutions de logiciels-services et de prix plafonds :
  - Y compris l’escompte, en pourcentage, applicable;
  - Les fournisseurs peuvent remplir le tableau de l’annexe C, ou fournir un lien vers un catalogue commercial de logiciels-services
- ✓ Les fournisseurs doivent fournir une justification des prix pour démontrer que les prix proposés sont équitables et raisonnables.
- ✓ Les fournisseurs ont maintenant la possibilité d’utiliser leur propre liste de prix et de produits en ligne et de la faire examiner par SPAC.

Le but premier est de minimiser les changements et d’accepter les listes de prix et produits et

5. Critères dévaluation normalisés (3/5)

Annexe C - Prix plafond des solutions et des services professionnels

Option 1: les fournisseurs fournissent un lien vers leur catalogue disponible enligne et indiquent le pourcentage de remise offert au GC.

Option 2: Les fournisseurs remplissent un tableau qui comprend la liste des produits et les prix plafonds pour les solutions SaaS ainsi que les services professionnels avec d'autres informations telles que les mesures des unités et le pourcentage de remise applicable.

5. Critères dévaluation normalisés (4/5)

Processus collaboratif d’évaluation

1

SPAC mènera l’évaluation des soumissions reçues en réponse à la DAMA **en collaboration avec les fournisseurs**. Si un fournisseur ne répond pas à tous les critères de qualification, on communiquera avec lui afin de lui demander des documents supplémentaires ou des précisions.

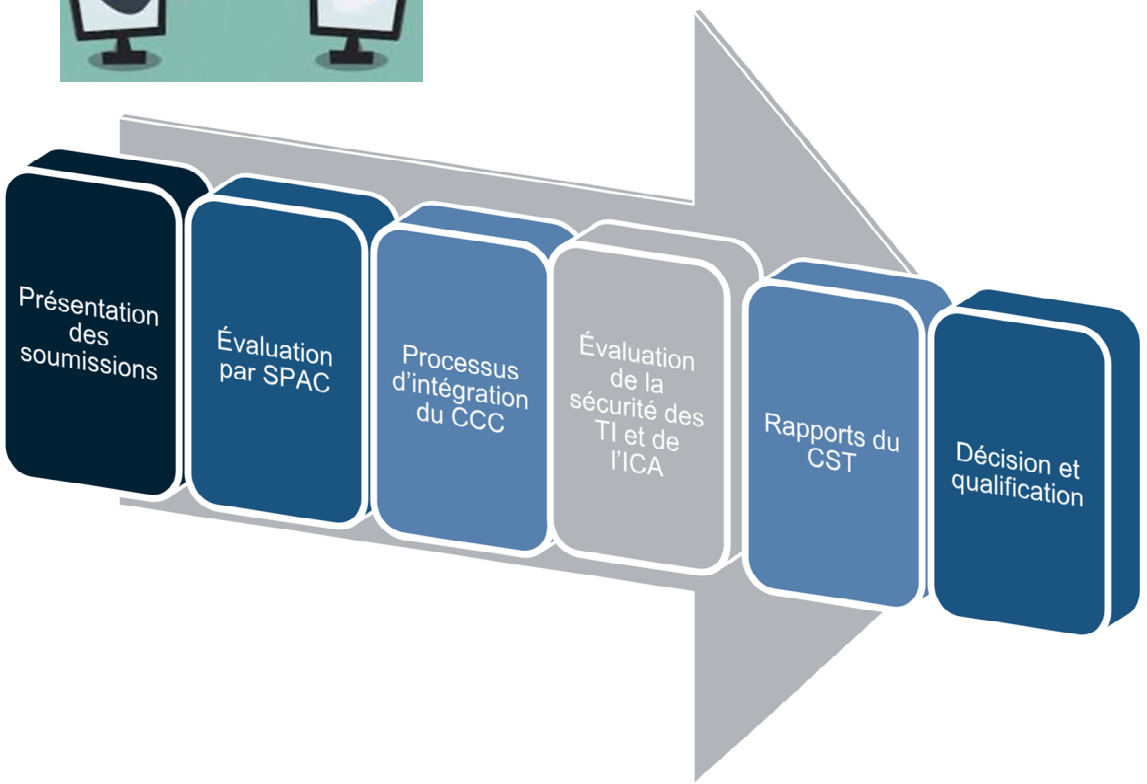
2

SPAC examinera les documents pour s’assurer que le fournisseur a bien soumis toute l’information requise. **L’objectif est de qualifier le plus grand nombre de fournisseurs possibles.**

3

SPAC évaluera les soumissions par rapport à tous les critères de qualification définis.

SPAC utilisera son entente avec le Centre canadien pour la cyber sécurité pour traiter **l’évaluation de l’ICA parallèlement à l’évaluation de la sécurité des TI.**



Nº de la DAMA sur Achatsetventes.gc.ca : EN578-191593/F

5. Critères dévaluation normalisés (5/5)

QUESTIONS? Communiquer avec nous !

Processus collaboratif pour soutenir votre soumission et votre candidature.

Pour des questions ou pour suggérer des révisions à la DAMA, les fournisseurs peuvent soumettre leurs commentaires ou questions à la boîte de réception de la DAMA: TPSGC.LENQS-SAAS.PWGSC@tpsgc-pwgsc.gc.ca

6. Évaluation de la sécurité des TI des SaaS (1/2)

Programme d'évaluation de la sécurité des TI :

Le Programme d'évaluation de la sécurité des TI des logiciels-services examine toutes les preuves disponibles pour satisfaire aux contrôles et aux améliorations de sécurité choisis par le GC avec un niveau d'assurance acceptable pour le stockage des données gouvernementales.

Les évaluations peuvent aussi s'appuyer sur les directives, les normes et les rapports du CST provenant du GC et des organismes alliés, sur les pratiques exemplaires de l'industrie et sur les certifications commerciales. L'utilisation de ces différentes ressources encouragera les fournisseurs de logiciels-services à interagir avec le GC, les vérificateurs tiers et les autres organismes d'évaluation afin de comprendre les capacités en matière de sécurité des TI et les risques résiduels des services infonuagiques utilisés par les ministères clients.

Intégrité de la chaîne d'approvisionnement (ICA) :

Le processus d'intégrité de la chaîne d'approvisionnement est réalisé à l'aide des renseignements demandés par le CST dans le formulaire 6. Le CST examinera, évaluera et analysera les renseignements disponibles dans le cadre d'une entente de non-divulgation. Le CST communiquera directement avec le fournisseur s'il a des questions relatives à l'évaluation.

À la fin du processus, un rapport de sécurité sera produit et le résultat sera communiqué au ministère utilisateur.

6. Évaluation de la sécurité des TI des SaaS (2/2)

Exigences de certification de sécurité

Le Canada a pris la décision opérationnelle de choisir les combinaisons suivantes de certifications industrielles pour protéger les données et les biens du Canada.

*Catégorie d'information - jusqu'à **Protégé B***
(éditeur du logiciel-service seulement)
Exigences relatives à la sécurité (annexe A de la DAMA)
- ISO/IEC 27001:2013
- ISO/IEC 27017:2015
- ISO/IEC 27018:2014
- Rapports des SOC 2 de type II
- ICA - Preuve de ISO/IEC 27036, **ou** Publication spéciale NIST 800-161, **ou** Contrôle de sécurité ITSG-33, **ou** contrôles CSA STAR pour soutenir les contrôles de gestion de la chaîne d'approvisionnement CSA CCM.
- Liste de tous les sous-processeurs.
- Inspection SPAC CST

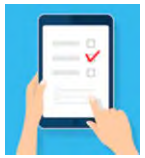
*Catégorie d'information - jusqu'à **Protégé A***
(Éditeur du logiciel-service et revendeur de produits modifiés)
Exigences relatives à la sécurité (annexe A de la DAMA)
- ISO/IEC 27001:2013 **ou**
- Rapports des SOC 2 de type II
- ICA - Preuve de ISO/IEC 27036, **ou** Publication spéciale NIST 800-161, **ou** Contrôle de sécurité ITSG-33, **ou** contrôles CSA STAR pour soutenir les contrôles de gestion de la chaîne d'approvisionnement CSA CCM.
- Liste de tous les sous-processeurs.
- Inspection SPAC CST

*** Les fournisseurs doivent également satisfaire aux critères obligatoires de sécurités de la DAMA et doivent fournir d'autres éléments obligatoire.**

7. Présentation de documents de tiers

Document	Palier 2 (Éditeur du logiciel-service - jusqu'à Protégé B)	Palier 1 (Éditeur du logiciel-service - jusqu'à Protégé A)	Palier 1 (Revendeurs de produits modifiés - jusqu'à Protégé A seulement)
Formulaire 1 - Formulaire de présentation de la soumission	X	X	X
Formulaire 2 - Formulaire d'attestation de l'éditeur de logiciels-services	X	X	
Formulaire 3 - Formulaire d'autorisation de l'éditeur de logiciels-services			X
OPTIONNEL : Formulaire 4 - Attestation aux fins du Programme de marchés réservés aux entreprises autochtones	X	X	X
Formulaire 5 - Liste de vérification de l'exhaustivité de la soumission	X	X	X
Formulaire 6 - Modèle de soumission d'intégrité de la chaîne d'approvisionnement (ICA)	X	X	
Annexe A - Exigences de qualification - Palier 1		X	X
Annexe A - Exigences de qualification - Palier 2	X		
Annexe C - Catalogue de solutions de logiciels-services et prix plafonds	X	X	X
Au besoin: Viabilité financière	X	X	X
Annexe D - Accords sur les niveaux de service (ANS)	X	X	X
Au besoin : Formulaires des Dispositions relatives à l'intégrité – déclaration de condamnation à une infraction	X	X	X

8. Comment participer (1/2)



Étape 1 : Téléchargez la DAMA, les modifications et les documents connexes :

- https://achatsetventes.gc.ca/donnees-sur-l-approvisionnement/appels-d-offres/PW-EEM-003-35660

Étape 2 : Sélectionnez le volet visé par votre soumission

- Éditeur de logiciels-services - jusqu'à Protégé A
- Revendeurs de produits modifiés - jusqu'à Protégé A seulement
- Éditeur de logiciels-services - jusqu'à Protégé B

Étape 3 : Préparez votre soumission (détails à la diapositive 15)

- Fournissez des artéfacts démontrant comment vous répondez aux exigences techniques, financières, de sécurité et d'intégrité de la chaîne d'approvisionnement
- Assurez-vous d'avoir les dernières certifications ISO et les derniers rapports de vérification
- Le processus de soumission implique également de remplir plusieurs formulaires requis par la DAMA.

Étape 4 : Envoyez votre soumission

- Option 1 : Connexion postel : https://www.canadapost.ca/cpc/fr/business/postal-services/digital-mail/epost-connect.page
- Option 2 : Courriel : TPSGC.LENQS-SAAS.PWGSC@tpsgc-pwgsc.gc.ca

Vous avez des difficultés? Communiquez avec nous TPSGC.LENQS-SAAS.PWGSC@tpsgc-pwgsc.gc.ca

8. Comment participer (2/2)

Résultats - Attribution d'AMA

Le fournisseur sera informé du résultat de la qualification par courriel.	Le fournisseur sera autorisé à vendre les produits de logiciels-services au moyen de l'arrangement d'approvisionnement en ligne aux ministères clients rapidement et facilement	Le fournisseur sera ajouté à la liste des fournisseurs qualifiés, accessible par tous les ministères clients	Le fournisseur pourra mettre à jour la liste des produits et les prix en avisant SPAC.

Vous avez des difficultés? Communiquez avec nous TPSGC.LENQS-SAAS.PWGSC@tpsgc-pwgsc.gc.ca

9. Comment les ministères achètent-ils des SaaS protégés au moyen de l'AMA?

Étape 1 :
Détermination de la ou des solutions de logiciels-services

- Déterminer la ou les solutions de logiciels-services et les services applicables en consultant le catalogue du GC ou autre.
- Rédiger l'énoncé des besoins (EB), le cas échéant.

Étape 2 :
Diffuser une demande de soumission simplifiée ou justifier le recours à un fournisseur unique

- Le client ou l'autorité contractante de SPAC diffusera une demande de soumissions simplifiée aux détenteurs de l'AMA qualifiés ou établira un contrat à fournisseur unique.
- Les soumissions des fournisseurs seront évaluées (le cas échéant).

Étape 3 :
Attribution et gestion du contrat

- Le contrat est signé avec le détenteur de l'AMA.
- L'utilisation des logiciels-services et les paiements sont gérés par le ministère client.

10. Sommaire de la présentation

- C'est la voie à suivre
- Impliquez-vous dans la transformation numérique du GC
- Augmentez votre présence sur le marché GC
- Processus qualification facile
- Tirer profit des connaissances de SPAC pour se qualifier
- Flexible et orienté vers l’entreprise
- Les départements sont impatients d'acheter
- Accessible aux municipalités, aux provinces, aux universités, etc.

FIN DE L'EXPOSÉ

Nº de la DAMA sur Achatsetventes.gc.ca : EN578-191593/F

QUESTIONS ET RÉPONSES

COMMENTAIRES

Information supplémentaire

LIMITATION DE RESPONSABILITÉ

Responsabilité de première partie

Exécution du contrat : L'entrepreneur est entièrement responsable de tous les dommages subis par le Canada, causés par l'exécution ou l'inexécution du contrat par l'entrepreneur.

Fuite de données : L'entrepreneur est entièrement responsable de tous les dommages subis par le Canada, causés par une infraction à la sécurité ou un manquement à l'obligation de confidentialité entraînant la consultation ou la divulgation non autorisée de dossiers, de données ou de renseignements appartenant au Canada ou à un tiers.

Limitation par incident : Sous réserve de la clause suivante, quel que soit le fondement ou la nature de la réclamation, la responsabilité totale par incident de l'entrepreneur n'excédera pas la valeur cumulative des factures liées au contrat au cours des douze (12) mois précédant l'incident.

Aucune limitation : La limitation de responsabilité susmentionnée de l'entrepreneur ne s'applique pas :

a) à toute inconduite volontaire ou à tout acte répréhensible délibéré;

b) à tout manquement aux obligations relatives à la garantie.

Responsabilité de tierce partie : Chaque partie convient qu'elle soit pleinement responsable des dommages qu'elle cause à un tiers dans le cadre du contrat, que la réclamation soit déposée par le tiers auprès du Canada ou de l'entrepreneur, ou des deux. Le montant de la responsabilité sera celui précisé dans l'accord conclu entre les parties ou déterminé par la cour. Les parties conviennent de se rembourser mutuellement tout paiement versé à un tiers en lien avec les dommages causés par l'autre partie et de rembourser rapidement leur part de responsabilité.