AUTORITÉ DES MARCHÉS PUBLICS | TRANSPARENCE ÉQUITÉ SAINE CONCURRENCE

Objet : Décision de l'Autorité des marchés publics concernant l'examen du processus de qualification identifié au SEAO sous le numéro de référence 20102824 – Services Internet spécialisés

Le 22 décembre 2025, une plainte est soumise à l'Autorité des marchés publics (AMP) concernant le processus de qualification mentionné en objet, publié le 29 octobre 2025 par le ministère de la Cybersécurité et du Numérique (MCN). L'ensemble des motifs énoncés dans cette plainte sont rejetés.

Conformément à l'article 37 de la *Loi sur l'Autorité des marchés publics*[1] (LAMP), le rôle de l'AMP est de déterminer si les documents de l'appel de qualification prévoient des conditions qui n'assurent pas un traitement intègre et équitable des concurrents, ne permettent pas à des concurrents d'y participer bien qu'ils soient qualifiés pour répondre aux besoins exprimés ou ne sont pas autrement conformes au cadre normatif[2].

L'examen réalisé par l'AMP lui permet de conclure que le MCN a agi, à l'égard des motifs soulevés dans la plainte, en conformité avec le cadre normatif applicable.

Plaintes et motifs

La plainte mentionne que les conditions prévues aux documents d'appel d'offres n'assurent pas un traitement intègre et équitable des concurrents, ne permettent pas à des concurrents qualifiés de participer dans des conditions claires et prévisibles et ne sont pas conformes au cadre normatif, notamment au regard de la *Loi sur les contrats des organismes publics*[3], du *Règlement sur les contrats des organismes publics en matière de technologies de l'information*[4] et de la *Loi sur l'Autorité des marchés publics*[5].

1- La grille d'exigences et d'évaluation (Annexe A) ne permet pas une évaluation objective des fournisseurs

La plainte mentionne plus précisément que les critères d'évaluation de l'Annexe A et de la section 1.8 ne sont pas clairement définis et manquent d'objectivité et de transparence. Au soutien de cette affirmation, il est indiqué que l'Annexe A (la Grille d'exigences des SIS) et la section 1.8 ne définissent pas des critères mesurables ni des modalités d'appréciation, barèmes, seuils ou pondération des critères. Puisque cette appréciation repose, selon le plaignant, sur une autodéclaration et des justificatifs non normalisés, il est affirmé que cette situation crée une subjectivité dans l'évaluation et un risque d'inégalité de traitement, qui est contraire aux principes de la LCOP.

[1] RLRQ, c. A-33.2.1.
[2] Tel que le prévoit l'article 69 LAMP, avec les adaptations nécessaires.
[3] RLRQ, c. C-65.1.
[4] RLRQ, c. C-65.1, r. 5.1.
[5] RLRQ, c. A-33.2.1.

L'annexe A des documents d'appel d'offres comporte 18 exigences, extraites du Devis technique, auxquelles le fournisseur doit répondre par « oui » ou par « non » afin d'indiquer s'il est en mesure de s'y conformer, en fournissant notamment des notes explicatives, des références et de la documentation technique au soutien de ses réponses.

Dans ses observations, le MCN a mentionné à l'AMP qu'il considère que les règles régissant l'évaluation des soumissions sont décrites de façon claire à l'Annexe A et permettent à plusieurs fournisseurs de se qualifier. Il est de plus indiqué que les exigences à respecter réfèrent à la maturité et à la capacité de ceux-ci de livrer des services Internet à haut débit de qualité dans les trois domaines couverts dans l'Annexe A (le volet technologique, les modalités de gestion et le cadre de sécurité). Le MCN affirme que les exigences du volet technologique de l'Annexe A visent à démontrer la capacité des infrastructures du réseau du fournisseur à assurer la continuité des services de qualité, alors que les exigences des modalités de gestion et de sécurité visent à exposer la maturité des processus du fournisseur pour livrer des services selon les attentes du MCN et de sa clientèle. Ainsi, il est considéré par le MCN que la plupart des justifications demandées sont de nature technique ou requiert de la documentation typique dans le domaine de la gestion des services, ce qui a pour effet de restreindre les interprétations possibles et la subjectivité lors de l'évaluation des soumissions. Enfin, il est prévu que trois ressources expertes du MCN dans le domaine des télécommunications seront assignées spécifiquement à l'analyse de ce volet des soumissions et qu'en cas de doutes, ces derniers pourront demander des explications additionnelles au fournisseur.

Au surplus, un travail d'adéquation entre les exigences retenues et le contenu du devis a été effectué afin d'éviter tout écart ou disparité dans les documents contractuels, de même qu'une analyse du marché et une veille afin de s'assurer que les exigences retenues n'aient pas pour effet de porter atteinte à la concurrence.

L'AMP est d'avis que le MCN a effectué une démarche sérieuse et documentée au soutien des exigences requises de l'Annexe A et que les conditions actuelles prévues permettent de procéder à une évaluation objective des fournisseurs, assurant une égalité de traitement des soumissions. De plus, trois ressources expertes effectueront l'évaluation de la conformité pour chacune des trois sections de l'Annexe A. De fait, l'AMP considère qu'aucun fournisseur ne serait désavantagé dans le cadre de l'appel de qualification et que cet élément est conforme au cadre normatif.

Pour les motifs 2, 3 et 4, la plainte indique que les sections 6.3, 6.4 et 6.5 du Devis technique ne permettent pas à plusieurs fournisseurs qualifiés de répondre à l'avis de qualification, qu'elles imposent des exigences disproportionnées et qu'elles sont inadaptées à un environnement multiclient et au réseau public. De fait, la plainte indique que ces obligations systémiques liées au transfert intégral des logs, à la déclaration de tout incident potentiel ainsi qu'aux délais de correction uniformes issus de la Directive[6], entraînent une charge excessive aux fournisseurs, des risques liés à la confidentialité ainsi que des coûts disproportionnés. Enfin, pour le plaignant, la sécurité est légitime, mais les moyens pour y parvenir doivent rester proportionnels et compatibles avec les environnements multiclient.

[6] *Directive gouvernementale de gestion des menaces, des vulnérabilités et des incidents*.

De façon globale, le MCN invoque quant à lui que sa mission est, entre autres, d'assurer la sécurité des services technologiques qu'il développe, exploite ou met à la disposition des organismes publics et des citoyens, conformément à la *Loi sur le ministère de la Cybersécurité et du Numérique*[7], et qu'à ce titre il exerce également un rôle central en matière d'encadrement de la cybersécurité à l'échelle gouvernementale en plus d'assurer, conformément à la *Politique de cybersécurité*[8], la détection, la coordination et la gestion des incidents de sécurité de l'information touchant l'administration publique et ses organismes.

De même, en vertu de *la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*[9], le MCN mentionne qu'il demeure pleinement responsable de la sécurité de l'information relative à ses actifs informationnels et aux services qu'il rend, incluant les exigences de confidentialité, d'intégrité et de disponibilité. Cette responsabilité subsiste intégralement, même lorsque certains volets des services technologiques sont confiés, impartis ou délégués à des fournisseurs ou à des prestataires de services externes; une telle délégation n'ayant pas pour effet de transférer la responsabilité ultime en matière de sécurité de l'information.

En conséquence, le MCN invoque qu'il est tenu d'énoncer, d'imposer et de faire respecter des exigences de sécurité de l'information dans le cadre de ses appels d'offres publics, appels de qualification et autres instruments contractuels, afin d'assurer la conformité aux obligations légales, réglementaires et gouvernementales applicables, ainsi qu'une gestion adéquate des risques dans les contrats qu'il octroie.

2- La section 6.3 Journaux de sécurité de l'information

Plus spécifiquement, la plainte invoque le référentiel NIST SP 800-92, qui préconise, selon le plaignant, une gestion proportionnée des journaux priorisant la pertinence, la rétention et la protection des données plutôt que leur transmission systématique. Il est de plus mentionné que cette façon de fonctionner favorise la collecte sélective, le filtrage et la corrélation, puisque ce sont des extraits ciblés et utiles qui sont partagés en cas d'incident. Enfin, la plainte demande qu'une modification des documents d'appel d'offres soit effectuée afin qu'un alignement sur le référentiel NIST SP 800-92 et la norme ISO/IEC 27035 1 :2023 soit requis, ce qui aurait pour conséquence qu'une disponibilité et une conservation des logs seraient effectuées par le fournisseur, mais qu'une transmission ciblée des extraits pertinents serait faite lors d'incidents avérés, audits ou demandes motivées avec pseudonymisation et chiffrement.

Le MCN, dans ses observations, mentionne quant à lui qu'il est tenu d'énoncer, d'imposer et de faire respecter des exigences de sécurité de l'information dans ses processus contractuels afin d'assurer la conformité aux obligations légales, réglementaires et gouvernementales qui lui sont applicables, de même qu'une gestion adéquate des risques.

[7] RLRQ c. M-17.1.1.
[8] Politique gouvernementale de cybersécurité du Québec.
[9] RLRQ, c. G-1.03.

Il indique que la détermination de ces exigences repose sur le cadre normatif[10] qui lui est applicable et sur les bonnes pratiques reconnues à l'échelle internationale[11], modulée selon la nature des services recherchés, leur niveau de criticité ainsi que de la sensibilité des informations qui seront traitées.

Plus spécifiquement, le MCN énonce que la journalisation exhaustive est une mesure de visibilité complète aux fins de détecter les cyberattaques et les abus de privilèges d'un usager légitime et que ce besoin repose sur trois piliers fondamentaux que sont l'imputabilité et la traçabilité, la détection précoce des comportements anormaux, de même que la conformité et la preuve. Ils servent d'appui à l'investigation lors d'un incident de sécurité.

Questionné quant à la compatibilité avec un environnement multiclient, le MCN affirme qu'une journalisation et la transmission de celle-ci sont possibles avec une architecture rigoureuse. Il ajoute que le principe de cloisonnement s'applique et est implanté dans ses solutions technologiques. La solution doit garantir que les journaux de chaque client ne sont jamais visibles par les autres. Pour cet avis de qualification, le MCN indique que les mesures de sécurité ont été allégées afin de répondre aux préoccupations des fournisseurs, que les transmissions sont ciblées et qu'il n'est pas nécessaire qu'elles soient reçues en temps réel, puisque le contexte d'affaires ne le requiert pas. Il sera requis de recevoir tous les journaux de sécurité lors d'audit ou d'incident de sécurité potentiel ou avéré.

L'AMP est d'avis que la section 6.3, telle que prévue, n'est pas susceptible d'affecter la concurrence et d'empêcher un fournisseur de se qualifier. Les besoins du MCN de disposer d'une architecture rigoureuse se justifient par ses diverses obligations gouvernementales, notamment quant à son besoin de pouvoir lier chaque action à une identité numérique unique grâce à la transmission ciblée des journaux. Cette démarche du MCN vise entre autres la détection de cyberattaque et l'obtention d'appui lors d'une potentielle investigation. Finalement, cet aspect ne fait pas partie de l'évaluation de la conformité liée à l'Annexe A.

3- La section 6.4 Gestion des incidents de sécurité de l'information

La plainte indique plus précisément que le référentiel ISO/IEC 27035 1 :2023 repose sur la détection, la qualification et l'évaluation de l'impact et sur une réponse proportionnée. Il est énoncé que les événements ne doivent pas être assimilés à des incidents avérés et que les référentiels mentionnés aux sections 6.3, 6.4 et 6.5 recommandent une transmission ciblée, de même que la qualification des incidents plutôt qu'une exhaustivité systématique des journaux ou encore la déclaration de faux

[10] Le MCN mentionne dans ses observations les lois, règlements, politiques et directives en vigueur au Québec, incluant notamment la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, telle que modifiée par la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* ainsi qu'un arrêté ministériel établissant une méthodologie obligatoire d'évaluation de la sensibilité de l'information, laquelle impose la classification des informations selon les préjudices potentiels qu'une atteinte à la confidentialité, à l'intégrité ou à la disponibilité pourrait entraîner, méthodologie à laquelle le MCN est tenu de se conformer dans l'exercice de ses fonctions.

[11] Les bonnes pratiques reconnues à l'échelle internationale mentionnées par le MCN incluent la norme ISO/IEC 27001, le cadre NIST SP 800-53 et le standard ITSG-33, adoptés respectivement par les gouvernements des États-Unis et du Canada.

positifs. Le plaignant demande que l'obligation de déclaration porte sur les incidents confirmés et classés avec une matrice de sévérité, et ce, conformément à la norme ISO/IEC 27035 1 :2023, car la déclaration de tous les potentiels, incluant les faux positifs, induit une surcharge aux fournisseurs et ne reflète pas les pratiques standard.

Dans le cadre de ses observations, le MCN indique que lors d'un incident de sécurité, il est fréquent que la confirmation d'une fuite de données ou d'un bris d'intégrité ne soit possible qu'après la réalisation d'investigations numériques et que les situations potentielles doivent, par conséquent, initier le processus de gestion des incidents de sécurité afin de confirmer ou d'infirmer la situation, assurant ainsi une prise en charge adéquate. Subséquemment, le MCN est d'avis que cet effort est requis afin d'assurer une prise en charge de tous les incidents de sécurité et que son expérience en la matière démontre que la majorité des signalements sont fondés. Finalement, il est allégué que cette exigence est présente sous une forme similaire depuis plus de dix ans.

De même, le MCN affirme que plus d'un fournisseur peut offrir une solution permettant la transmission de ces signalements et précise qu'il détient également une solution, si requise. Se disant agile sur la méthode de signalement de l'incident et de transmission des journaux (ou autres preuves), le MCN est d'avis que tous les fournisseurs sont en mesure d'effectuer la transmission requise, considérant la simplicité et la versatilité des options offertes. Enfin, le MCN n'exige pas et ne prévoit pas exiger que les signalements d'incidents soient faits de façon automatique.

L'AMP est d'avis que la formulation, telle que proposée à la section 6.4 du Devis technique, n'est pas de nature à empêcher les fournisseurs potentiels de déposer une soumission ni de se qualifier. Les mesures mises en place par le MCN et les diverses possibilités offertes aux fournisseurs de transmettre les signalements répondent à un besoin réel du MCN et ne sont pas déraisonnables. De fait, la majorité des signalements d'incidents sont fondés et, par conséquent, le signalement d'événements potentiels est pertinent pour initier le processus de gestion des incidents de sécurité afin d'assurer une prise en charge adéquate. Finalement, la section 6.4 du Devis technique ne fait pas partie de l'évaluation de la conformité dans l'Annexe A.

4- La section 6.5 Gestion des vulnérabilités techniques

La plainte mentionne de façon plus spécifique que la section 6.5 amène le fournisseur à avertir le MCN s'il découvre une vulnérabilité dans l'infrastructure des « SIS » et à produire un plan de redressement en fonction des risques et du niveau de criticité associé à la vulnérabilité. Or, la publication des vulnérabilités du fournisseur pourrait mettre en péril la sécurité du service Internet pour l'ensemble de ses clients. Le plaignant allègue que le cadre gouvernemental établit que les processus et les rôles sont précisés, mais qu'aucune obligation de transfert exhaustif des journaux n'existe. Le plaignant demande qu'une matrice de risques (critique/majeur/mineur) des délais différenciés compatibles au cadre gouvernemental et à l'environnement multiclient soit mise en place, ainsi qu'une preuve d'impact public pour tout délai plus strict, sans quoi les fournisseurs seraient pénalisés, ce qui aurait pour effet de réduire la concurrence.

Dans ses observations, le MCN allègue qu'il n'y a pas d'enjeux pour les fournisseurs à divulguer les vulnérabilités de l'infrastructure et qu'il fait preuve de confidentialité dans leur traitement; ce ne sont que les vulnérabilités qui impactent le MCN ou ses clients qui sont visés. De plus, il indique que

le fournisseur ne peut pas évaluer les risques pour le MCN et ses clients, puisqu'il ne sait pas la nature des informations qui sont transmises par ces équipements. Par conséquent, il ne serait pas possible de fournir une matrice de risques plutôt que de divulguer les vulnérabilités. Enfin, le MCN allègue que cette exigence est présente sous une forme similaire depuis plus de dix ans.

Quant au besoin soutenant cette exigence, le MCN affirme qu'il est requis, pour éviter des cyberattaques, de s'assurer que les vulnérabilités décelées soient corrigées rapidement, particulièrement lorsqu'il s'agit de fournisseurs en télécommunication. Le MCN allègue que le Centre canadien pour la cybersécurité émet d'ailleurs fréquemment des avis à ce sujet. Ainsi, la section énonce les délais attendus.

L'AMP est d'avis que le processus de gestion des vulnérabilités permet d'assurer un durcissement des configurations, puisqu'il identifie et vise à corriger les vulnérabilités avant l'exploitation de ses failles, le tout basé sur un cadre de référence pour les meilleures pratiques de gestion des technologies de l'information. Il s'agit d'un besoin légitime du MCN, notamment au regard de ses responsabilités. Le fournisseur doit donc avertir le MCN dans les plus brefs délais s'il découvre une vulnérabilité dans l'infrastructure des « SIS » et produire un plan de redressement en fonction des risques et du niveau de criticité associé à la vulnérabilité. De plus, les réponses du MCN quant au traitement confidentiel des informations soumises dans le cadre de la divulgation des vulnérabilités de l'infrastructure satisfont l'AMP, notamment au niveau de la compatibilité avec un environnement multiclient. Par ailleurs, le MCN convainc l'AMP qu'il ne serait pas possible de la substituer par une matrice de risques tel que suggéré par la plainte, car la divulgation des vulnérabilités est nécessaire dans le cadre du processus de gestion des vulnérabilités et du plan de redressement. Enfin, l'AMP considère que la section 6.5, telle que formulée actuellement, n'a pas pour effet d'impacter la concurrence indûment ni de pénaliser indûment les fournisseurs potentiels.

5- L'absence de données volumétriques et d'informations claires quant au chevauchement contractuel entre le contrat découlant de l'appel d'offres SMP volet D et les contrats qui découleront de l'avis de qualification ne permettent pas la transparence et un traitement intègre et équitable des concurrents

Plus spécifiquement, le plaignant est d'avis que le MCN ne peut pas invalider les arguments qu'il lui a soumis portant sur l'absence de volumétrie ou de clarté en prétendant qu'ils relèvent d'un processus antérieur, puisque ces données constituent la base indispensable pour l'évaluation des risques, des coûts et de l'implantation opérationnelle dans le processus actuel. L'exigence imposée aux nouveaux fournisseurs de financer en amont des outils et des processus sans garantie de volume combiné à l'absence de données volumétriques et de règles claires quant au chevauchement contractuel entre le contrat découlant de l'appel d'offres SMP volet D et l'avis de qualification, crée une barrière à l'entrée et confère un avantage indu au fournisseur en place déjà titulaire du contrat SMP. Selon le plaignant, cette absence de transparence contrevient au principe de traitement intègre et équitable des concurrents et se manifeste également lorsque le MCN, malgré les questions précises des fournisseurs, se limite à faire référence aux documents déjà existants sans fournir de clarifications opérationnelles supplémentaires. Cette absence de précisions compromet la planification des fournisseurs et accentue les ambiguïtés.

Enfin, le plaignant est d'avis que certains aspects, notamment la formation, le transfert de connaissances et le délai de correction des vulnérabilités, manquent de clarifications (addendas 5 et 7).

Dans ses observations, le MCN précise que la volumétrie concernant l'appel d'offres SMP (SEAO 1508865) prévoyait l'acquisition de 245 liens « SIS ». Les nouveaux besoins recensés en 2024 et 2025 représentent plus de 2000 liens « SIS ». Concernant la simultanéité du contrat SMP et des futures demandes de prix, le MCN mentionne que le contrat découlant de l'appel d'offres SMP sera respecté dans sa totalité[12] et que les demandes de prix de l'avis de qualification seront émises une fois que les quantités disponibles dans le volet D du contrat SMP seront rencontrées. Comme il n'offre que 245 liens et qu'un avenant pour augmenter ce nombre à plus de 2000 serait non accessoire, l'appel de qualification vise à combler cet écart.

Questionné quant à la variation de la volumétrie, le MCN a précisé qu'elle varie effectivement en fonction du fournisseur, car c'est lui qui détermine la liste des produits technologiques mise en œuvre. Pour ce qui est de la volumétrie des journaux, le MCN indique qu'elle varie quelque peu d'un fabricant de produit à l'autre, mais que les proportions demeurent relativement similaires.

En ce qui concerne les réponses élaborées dans l'addenda 7, le MCN précise que la formation et le transfert de connaissances sont établis en fonction des requis des services (types, caractéristiques, configurations, normes, etc.) et de leur exploitation, lesquels sont fournis par le MCN dans l'appel de qualification et les demandes de prix. En conséquence, les fournisseurs seront bien au courant des attentes du MCN sur les thèmes et les éléments à couvrir. Les activités d'arrimage prévues à la suite de la signature du premier contrat du fournisseur permettront de préciser le contenu détaillé et le format requis pour le transfert des connaissances.

Pour ce qui est des délais de correction des vulnérabilités, le MCN mentionne qu'il est primordial que celles qui ont été détectées soient corrigées en priorité, notamment aux fins de se protéger contre ces cyberattaques.

Questionné quant à savoir si les modalités et exigences définies sont uniformes pour tous les fournisseurs, le MCN précise que le Devis technique unique établit un cadre commun d'exigences qui s'applique uniformément à l'ensemble des fournisseurs, sans distinction. À cet égard, les exigences sont conçues et appliquées selon :

- les principes de neutralité technologique basés sur les résultats attendus et non en fonction de moyens techniques spécifiques;
- des niveaux de service (SLA) standardisés : les délais de correction des vulnérabilités sont intégrés au tronc commun contractuel et s'imposent de manière identique à l'ensemble des fournisseurs, sans exception. Ils sont alignés sur les principaux référentiels reconnus, notamment ISO/IEC 27001, ITSG-33 et SOC 2;
- des mécanismes de validation de l'uniformité, autant par le processus d'appel de qualification que la matrice de conformité déposée par le fournisseur qui atteste de sa conformité aux obligations du devis.

[12] Le contrat SMP est d'une durée maximale de dix ans, soit cinq ans ferme, une option de renouvellement de trois ans et une période de transition à la sortie de deux ans. La date de fin du contrat est le 17 juillet 2032.

L'AMP est d'avis que le MCN a fait preuve d'une transparence suffisante quant aux informations transmises à l'appel de qualification en regard du processus qui sera applicable, notamment quant à la coexistence du contrat SMP volet D et les demandes de prix qui découleront de l'appel de qualification. De surcroît, la gestion entre le contrat SMP et les contrats résultant des demandes de prix futures n'a pas à être précisée actuellement. Cette stratégie d'acquisition n'empêche pas les fournisseurs de se qualifier et n'est pas susceptible de porter atteinte au traitement intègre et équitable des concurrents. Ainsi, aucun fournisseur n'est avantagé quant à sa capacité à se qualifier dans le cadre de l'avis de qualification. De plus, les informations actuellement disponibles ne sont pas susceptibles de créer une barrière à l'entrée ni de conférer un avantage indu au fournisseur en place déjà titulaire du contrat SMP. Le MCN a fait le choix de procéder par demandes de prix et celles-ci viendront préciser toutes les variables requises en temps opportun. C'est à ce moment que le besoin à combler sera clairement détaillé.

6- L'absence d'une méthode de mesure uniforme à la section 5.2.4 Gestion de la capacité et de la performance du devis technique impacte la concurrence et le traitement intègre et équitable des concurrents

Plus spécifiquement, le plaignant affirme qu'il est mentionné à la section 5.2.4. que les mesures de performance (la latence, la gigue et la perte de paquets) servent à démontrer l'atteinte des niveaux de services. Les mesures de performance doivent être fournies pour chaque point de présence (POP) utilisé par le fournisseur pour livrer les « SIS ». L'absence d'une méthode de mesure uniforme pour l'ensemble des fournisseurs n'assure pas un traitement intègre et équitable des concurrents.

Questionné quant à cet élément, le MCN mentionne que le fournisseur doit faire les mesures de performance en tout temps et avec un échantillonnage précis dans son réseau de transport entre ses points de présence (POP) et les points d'échange Internet. Par la suite, il doit produire un rapport mensuel démontrant l'atteinte des niveaux de performance exigés dans le Tableau 11 du Devis technique. Le MCN affirme que le Devis technique regroupe tous les critères et les exigences communs à l'ensemble des services « SIS » à acquérir. La demande de prix viendra, quant à elle, préciser les caractéristiques spécifiques des services. La section 7.2.1 du Devis technique fournit une liste exhaustive de ces dernières.

De même, le MCN est d'avis que les attentes sont claires pour les fournisseurs, puisque les exigences s'appuient sur des recommandations du Conseil de la radiodiffusion et des télécommunications canadiennes et des requis standards dans les offres commerciales des services Internet d'affaires.

L'AMP est d'avis que l'absence d'une méthode de mesure uniforme pour l'ensemble des fournisseurs à la section 5.2.4 ne porte pas atteinte au traitement intègre et équitable des concurrents et n'est pas susceptible d'empêcher des fournisseurs de se qualifier. Le MCN a fourni, notamment dans le Devis technique, des critères et des exigences qui sont communs à l'ensemble des services « SIS » à acquérir et le niveau de service voulu à rencontrer. De plus, les renseignements spécifiques et pertinents seront partagés aux fournisseurs au moment du dépôt des demandes de prix. Il est donc de la responsabilité du fournisseur de se doter des moyens nécessaires et des mécanismes appropriés pour s'assurer qu'il fait une gestion adéquate de la capacité. Par ailleurs, l'AMP rappelle que la gestion de la capacité et de la performance ne seront pas directement évalués dans le cadre de la qualification.

Analyse

Les organismes publics bénéficient d'une grande latitude lorsqu'ils déterminent les exigences qu'ils incluent dans la documentation au soutien de leurs processus contractuels. Cette latitude demeure toutefois sujette aux principes voulant que ces exigences soient conformes au cadre normatif, liées aux besoins déterminés et édictées de bonne foi.

Considérant l'ensemble des éléments qui précèdent, l'AMP conclut que la plainte et ses motifs doivent être rejetés. En effet, à la suite de l'analyse des allégations soulevées, l'AMP est d'avis que les conditions et exigences prévues aux documents de l'appel de qualification du MCN ne briment pas le traitement intègre et équitable des concurrents, n'empêchent pas un concurrent de participer au processus bien qu'il soit qualifié pour se faire, ni ne sont autrement contraires au cadre normatif. Veuillez noter que la présente décision est finale et sans appel.