C A N A D A

PROVINCE DE QUÉBEC
DISTRICT DE MONTRÉAL

R É G I E D E L ' É N E R G I E

NO : R-3929-2015

HYDRO-QUÉBEC, personne morale de droit public légalement constituée en vertu de la *Loi sur Hydro-Québec* (L.R.Q. c. H-5) ayant son siège social au 75, René-Lévesque Ouest, dans la cité et district de Montréal, province de Québec

Demanderesse

DEMANDE DU TRANSPORTEUR POUR LA CRÉATION D'UN COMPTE DE FRAIS REPORTÉS POUR L'IMPLANTATION ET L'APPLICATION DE LA VERSION 5 DES NORMES DE PROTECTION DES INFRASTRUCTURES CRITIQUES DE LA NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

[Articles 31(5˚) et 32 de la *Loi sur la Régie de l'énergie* (L.R.Q. c. R-6.01)]

AU SOUTIEN DE SA DEMANDE, LA DEMANDERESSE EXPOSE RESPECTUEUSEMENT CE QUI SUIT :

1. Elle est une entreprise dont les activités de transport d'électricité sont assujetties à la juridiction de la Régie de l'énergie (la « Régie ») dans la mesure prévue à la *Loi sur la Régie de l'énergie* (la « Loi »).

2. Hydro-Québec dans ses activités de transport d'électricité (le « Transporteur ») a pour mandat, entre autres, de développer et d'exploiter le réseau de transport de façon à satisfaire les besoins des clients tout en assurant la pérennité et la fiabilité du réseau.

3. Le Transporteur entreprend des démarches et travaux relatifs à l'implantation et l'application de la version 5 des normes de protection des infrastructures critiques (« normes CIP v5 ») de la North American Electric Reliability Corporation (la « NERC »).

4. Les normes de protection des infrastructures critiques (« CIP ») visent l'identification et la sécurisation des actifs électroniques BES[1] pouvant entraîner un impact sur l'exploitation fiable du réseau de transport principal. Les normes CIP v5 concernent notamment le rehaussement des mécanismes de sécurité, la formation du personnel, la gestion de la sécurité ainsi que le plan de rétablissement en cas d'incidents, le tout

[1] Actifs électroniques BES (*Bulk Electric System*) : définition selon le *Glossaire des termes en usage dans les normes de fiabilité de la NERC*, mais appliquée au réseau de transport principal (RTP).

tel que plus amplement décrit à l'annexe A des présentes intitulée *Sommaire de la version 5 des normes de protection des infrastructures critiques de la North American Electric Reliability Corporation.*

5. La version 5 des normes CIP préconise une nouvelle méthodologie pour inventorier et catégoriser les systèmes électroniques BES et leurs actifs électroniques connexes en fonction de leur impact élevé, moyen ou faible sur la fiabilité du réseau de transport principal. Le Transporteur prévoit une augmentation du nombre de ses actifs électroniques d'environ 12 000, pour les centres d'exploitation du réseau et les postes de transport, par rapport à la version 3 des normes CIP qui est actuellement appliquée par le Transporteur et en vigueur aux États-Unis.

6. Le Transporteur, comme la plupart des juridictions voisines, se prépare à l'implantation et l'application des normes CIP v5 au 1er avril 2016. Ainsi, le Transporteur concentre ses efforts afin de rendre conformes ses systèmes électroniques BES ayant un impact élevé et moyen sur la fiabilité du réseau de transport principal d'ici cette date.

7. La conformité du réseau de transport aux normes CIP v5 de la NERC est requise pour assurer l'uniformité de la version des normes CIP appliquée à l'échelle de l'Amérique du Nord. Le Transporteur a par conséquent dû entreprendre certaines activités afin d'assurer la conformité de ses installations aux normes CIP v5 pour le 1er avril 2016.

8. Le Transporteur demande l'approbation de la Régie pour la création d'un compte de frais reportés, notamment pour les motifs suivants :

- Aucune charge relative aux activités énumérées au point 10 ci-dessous n'a été incluse au dossier tarifaire 2015 du Transporteur ;

- Le Coordonnateur de la fiabilité déposera sous peu auprès de la Régie une demande d'adoption des normes CIP v5, à la suite du processus de consultation publique tel que décrit à l'annexe de la décision D-2011-139, qui s'est terminé en avril 2015 ;

- Le Transporteur connaît maintenant avec plus de précision les activités nécessaires et les coûts inhérents à l'implantation des normes CIP v5 ;

    - Dans le contexte de l'implantation des normes CIP v5, la NERC et la Federal Energy Regulatory Commission ont précisé au cours de 2014 et précisent encore la manière dont les ressources humaines et technologiques et les processus doivent évoluer de manière à permettre la conformité à cette version des normes ;

    - Le Transporteur a réalisé au cours de 2014 et a poursuivi en 2015 l'analyse des solutions technologiques à déployer pour se conformer aux exigences des normes CIP v5 ;

- Ce dernier doit réaliser un volume d'activités important dont les coûts sont élevés, compte tenu de l'augmentation du nombre d'actifs visés du Transporteur.

9. Les charges pour les activités entreprises par le Transporteur en 2015, liées aux systèmes électroniques BES catégorisés comme ayant un impact élevé ou moyen sur la fiabilité du réseau de transport principal, s'élèvent à environ 7 M$.

10. Les principales activités non récurrentes d'implantation sont les suivantes :

- Identification et catégorisation initiales des systèmes électroniques BES ;
- Rehaussement des périmètres de sécurité électroniques pour se conformer aux exigences des normes CIP v5 concernant les points d'accès, la gestion des accès et le contrôle des flux de données ;
- Rehaussement des contrôles des accès électroniques et physiques aux systèmes électroniques BES ;
- Mise en place de mesures compensatoires, notamment pour la gestion des changements de configuration et la gestion des accès avant le déploiement de solutions technologiques ;
- Normalisation et déploiement de l'architecture des technologies de l'information et de ses composants pour permettre une gestion des changements de configuration efficace et efficiente.

11. Le Transporteur demande à la Régie l'autorisation de créer un compte de frais reportés, hors base, portant intérêts, et dont les modalités de disposition seront approuvées ultérieurement par la Régie dans le cadre de la demande tarifaire 2016.

12. Le Transporteur demande l'autorisation d'inscrire dans ce compte de frais reportés, les frais réels engagés pour 2015, et ce pour reconnaissance ultérieure dans les tarifs de transport d'électricité, selon les modalités de disposition prévues au paragraphe précédent.

13. La présente demande n'est pas visée par l'article 25 de la Loi et, conséquemment, ne requiert pas une audience publique.

14. La présente demande est bien fondée en faits et en droit.

PAR CES MOTIFS, PLAISE À LA RÉGIE :

ACCUEILLIR la présente demande ;

ACCORDER au Transporteur l'autorisation requise selon la Loi, pour la création d'un compte de frais reportés, hors base et portant intérêts, relatif à l'implantation et l'application, aux installations du Transporteur, de la version 5 des normes de protection des infrastructures critiques de la North American Electric Reliability Corporation afin d'y comptabiliser les frais réels engagés à cette fin pour 2015.

Montréal, le 5 juin 2015

(S) Affaires juridiques Hydro-Québec

Affaires juridiques Hydro-Québec
(Me Yves Fréchette)

Annexe A
Sommaire de la version 5 des normes de protection des infrastructures critiques de la North American Electric Reliability Corporation

CIP-002-5.1 : Cybersécurité – Catégorisation des systèmes électroniques BES

Cette norme exige d'inventorier et de catégoriser les systèmes électroniques BES et leurs actifs électroniques BES connexes, en fonction de critères spécifiques pour l'application des exigences de cybersécurité proportionnelle à l'impact négatif que la perte, la dégradation ou la mauvaise utilisation de ces systèmes électroniques BES pourrait avoir sur l'exploitation fiable du BES. L'inventaire et la catégorisation des systèmes électroniques BES permettent d'établir une protection appropriée contre les dégradations qui pourraient entraîner un fonctionnement incorrect ou une instabilité du BES.

CIP-003-5 : Cybersécurité – Mécanismes de gestion de la sécurité

Cette norme exige des entités responsables qu'elles définissent des mécanismes de gestion de la sécurité cohérents et viables qui établissent les responsabilités et l'imputabilité à l'égard de la protection des systèmes électroniques BES contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou des instabilités dans le BES. Plusieurs politiques de cybersécurité (par exemple, personnel et formation, périmètres de sécurité électronique, plans de rétablissement des systèmes électroniques, gestion des changements de configuration et analyses de vulnérabilité) doivent être mises en œuvre et l'entité responsable doit confier à un cadre supérieur CIP la responsabilité de mener et de gérer l'implantation et le respect permanent des normes CIP.

CIP-004-5.1 : Cybersécurité – Personnel et formation

Cette norme vise à minimiser les risques de compromissions, qui pourraient entraîner un fonctionnement incorrect ou une instabilité du BES, attribuables à des personnes qui accèdent à des systèmes électroniques BES, en exigeant la gestion des accès, une évaluation des risques liés au personnel, une formation et une sensibilisation à la sécurité qui soient adéquates pour protéger ces systèmes électroniques BES.

CIP-005-5 : Cybersécurité – Périmètres de sécurité électronique

Cette norme impose aux entités responsables de gérer l'accès électronique aux systèmes électroniques BES en établissant un périmètre de sécurité électronique (ESP) contrôlé afin de protéger les systèmes électroniques BES contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou une instabilité dans le BES. Le contrôle des flux entrants et sortants du périmètre de sécurité électronique et la gestion des accès distants interactifs à l'aide d'authentification multifactorielle sont des exemples d'exigences que l'on trouve dans cette norme.

CIP-006-5 : Cybersécurité – Sécurité physique des systèmes électroniques BES

Cette norme vise à gérer l'accès physique aux systèmes électroniques BES en établissant un plan de sécurité physique afin de protéger les systèmes électroniques BES contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou une instabilité dans le BES. Par exemple, l'utilisation de cartes d'accès, les systèmes de verrouillage, le personnel de sécurité et les dispositifs d'authentification tels que les systèmes de lecteurs de carte d'accès et de saisie de code d'accès [numéro d'identification personnel (NIP)] sont autant de méthodes utilisées pour assurer la sécurité physique des actifs

électroniques. La mise en place d'un programme de contrôle d'accès des visiteurs et d'un programme de maintenance et d'essai des systèmes de contrôle d'accès physiques sont également requis.

CIP-007-5 : Cybersécurité – Gestion de la sécurité des systèmes

Cette norme vise à gérer la sécurité des systèmes en établissant des exigences techniques, opérationnelles et administratives particulières afin de protéger les systèmes électroniques BES contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou une instabilité dans le BES. Par exemple, les entités responsables doivent avoir en place un processus permettant la gestion des ports et services, des rustines de sécurité et des logiciels pour la protection contre le code malveillant. De plus, des processus documentés doivent être prévus pour la surveillance des incidents de sécurité et la gestion des comptes d'accès logiques.

CIP-008-5.1 : Cybersécurité – Déclaration des incidents et planification des mesures d'intervention

Cette norme vise à réduire les risques posés au fonctionnement fiable du BES par un incident de cybersécurité en définissant des exigences d'intervention en cas d'incident. Un plan d'intervention en cas d'incidents de cybersécurité doit être établi, et tous les incidents doivent être documentés.

CIP-009-5 : Cybersécurité – Plans de rétablissement des systèmes électroniques BES

Cette norme définit les exigences relatives aux plans de rétablissement en vue du maintien de la stabilité, de l'exploitabilité et de la fiabilité du BES. Par exemple, les entités responsables doivent avoir instauré des plans de rétablissement des systèmes électroniques BES qui seront soumis à un exercice annuel.

CIP-010-1 : Cybersécurité – Gestion des changements de configuration et analyses de vulnérabilité

Cette norme vise à prévenir et détecter les changements non autorisés aux systèmes électroniques BES au moyen d'exigences relatives à la gestion et à la surveillance des changements de configuration. De plus, des analyses de vulnérabilité doivent être réalisées en vue d'identifier et de corriger les lacunes ciblées.

CIP-011-1 : Cybersécurité – Protection de l'information

Cette norme vise à empêcher tout accès non autorisé à l'information de système électronique BES en définissant des exigences de protection de l'information visant à prévenir toute compromission pouvant entraîner un fonctionnement incorrect ou une instabilité dans le BES. De plus, un processus documenté doit être prévu pour la réutilisation et l'élimination sécuritaire d'un actif électronique BES qui contient de l'information de système électronique BES dans le but d'empêcher la diffusion non autorisée d'information.

AFFIRMATION SOLENNELLE

Je, soussignée, **STÉPHANIE CARON**, chef, Affaires réglementaires et tarifaires, pour la division Hydro-Québec TransÉnergie, au 2, Complexe Desjardins, 19e étage, en la ville de Montréal, province de Québec, affirme solennellement ce qui suit :

1. La présente demande du Transporteur a été préparée en partie sous ma supervision et mon contrôle ;

2. J'ai une connaissance personnelle des faits relatifs à la réglementation et à la tarification du Transporteur allégués dans la présente demande ;

3. Tous les faits relatifs à la réglementation et à la tarification du Transporteur allégués à la demande d'autorisation sont vrais.

Et j'ai signé à Montréal, Québec,
Ce 5 juin 2015

(s) Stéphanie Caron

Stéphanie Caron

Déclaré solennellement devant moi,
à Montréal, Québec, ce 5 juin 2015

(S) Lucie Gauthier

Lucie Gauthier, avocate

AFFIRMATION SOLENNELLE

Je, soussignée, **CHRISTIANE SIMARD**, chef, Soutien Automatismes, direction Plans et soutien opérationnel, vice-présidence Exploitation des installations pour la division Hydro-Québec TransÉnergie, au 5250 rue Armand-Frappier en la ville de Saint-Hubert, province de Québec, affirme solennellement ce qui suit :

1. La présente demande du Transporteur a été préparée en partie sous ma supervision et mon contrôle ;

2. J'ai une connaissance personnelle des activités d'implantation du Transporteur alléguées dans la présente demande ;

3. Tous les faits relatifs aux activités d'implantation du Transporteur allégués à la présente demande sont vrais.

Et j'ai signé à Montréal, Québec,
Ce 5 juin 2015

(s) Christiane Simard

Christiane Simard

Déclaré solennellement devant moi,
à Montréal, Québec, ce 5 juin 2015

(S) Lucie Gauthier

Lucie Gauthier, avocate