Informations relatives aux normes

Projet QC-2019-05

Norme *CIP-003-8 – Cybersécurité – Mécanisme de gestion de la sécurité*

1. PRÉSENTATION DE LA NORME

1.1. Applicabilité de la norme

La norme CIP-003-8 s'applique aux fonctions visées suivantes :

- *Exploitant d'installation de production* (*GOP*)
- *Propriétaire d'installation de production* (*GO*)
- *Responsable de l'équilibrage* (*BA*)
- *Coordonnateur de la fiabilité* (*RC*)
- *Exploitant de réseau de transport* (*TOP*)
- *Propriétaire d'installation de transport* (*TO*)
- Certains *distributeurs* (*DP*)

Les *installations* visées sont :

- Les *installations* du *RTP* qui répondent aux critères définis dans la section Applicabilité.
- Certaines installations spécifiques des *distributeurs*.[1]

1.2. Objet de la norme

L'objectif de la norme CIP-003 est de définir les mécanismes de gestion de la sécurité 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 *système de production-transport d'électricité* (*BES*).

1.3. Contexte réglementaire

Actuellement, la norme en vigueur au Québec est la norme CIP-003-6. La Régie de l'énergie (ci-après appelée la « Régie ») a adopté la norme CIP-003-7 et son Annexe QC dans la décision D-2019-033[2]. La norme entrera en vigueur le 1er janvier 2020.

La norme CIP-003-8 a été adoptée par le conseil d'administration de la NERC le 9 mai 2019 et approuvée par la FERC le 31 juillet 2019 dans le cadre du dossier RD19-5-000[3].

[1] Voir la section Applicabilité des normes CIP pour les détails concernant l'application pour les distributeurs.
2. Régie de l'énergie, Décision D-2010-033, consultée le 8 octobre 2019 au http://publicsde.regie-energie.qc.ca/projets/461/DocPrj/R-4050-2018-A-0014-Dec-Dec-2019_03_15.pdf
3 FERC, Docket No. RD19-5-000, consulté le 8 octobre 2019 au https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/RD19-5-000%20Letter%20Order%20CIP-003-8.pdf (en anglais seulement)

1.4. Dispositions particulières pour le Québec

Le *Coordonnateur de la fiabilité* (ci-après appelé le « Coordonnateur ») propose de reconduire les spécificités québécoises, notamment le champ d'application et les dispositions particulières, déjà adoptées par la Régie dans sa décision D-2016-119 qui exempte certaines centrales et leur poste élévateur. La norme s'applique aux installations du *réseau de transport principal* (*RTP*) et aux installations spécifiées pour les *distributeurs*. De plus, les dispositions particulières suivantes s'appliquent

- Est exemptée de cette norme toute installation de production qui répond aux deux conditions suivantes : (1) la puissance nominale de l'*installation* est de 300 MVA ou moins et (2) aucun groupe de l'*installation* ne peut être synchronisé avec un réseau voisin.
- Sont exemptés de cette norme les postes élévateurs des *installations* de production exemptées selon le point précédent.

1.5. Dates d'entrée en vigueur proposées

La norme CIP-003-8 entrera en vigueur aux États-Unis le 1er avril 2020. Le plan de mise en œuvre aux États-Unis[4] précise que le délai entre l'approbation réglementaire et la mise en application de la norme doit être de six mois.

Au Québec, le Coordonnateur propose le même délai de six mois entre l'adoption de la norme par la Régie et son entrée en vigueur.

1.6. Normes ou exigences à retirer

La norme CIP-003-7 doit être retirée dès l'entrée en vigueur de la norme CIP-003-8.

1.7. Modifications au Glossaire

Les définitions proposées au Glossaire dans le cadre du dossier R-4070-2018 pour les termes « automatismes de réseau » et « plan de défense » sont reconduites au Glossaire afin d'assurer que la norme NERC puisse faire l'objet d'une interprétation cohérente.

2. ÉVALUATION DE LA PERTINENCE

Les modifications apportées à l'alinéa 5.2 de l'annexe 1 de la norme CIP-003-8 répondent aux objectifs de l'ordonnance nº 843[5] de la FERC, notamment sa préoccupation selon laquelle les entités visées doivent mettre en œuvre des contrôles pour atténuer le risque lié au code malveillant pouvant provenir des actifs électroniques temporaires des tiers. Ces modifications sont tout aussi pertinentes au Québec qu'ailleurs en Amérique du Nord.

Conformément à l'entente conclue en 2009 entre la Régie, la NERC et le NPCC et avec l'autorisation du gouvernement du Québec[6], cette norme a été élaborée et approuvée par des organismes externes pour l'Amérique du Nord, y compris le Québec. Le *coordonnateur de la fiabilité* est d'avis que cette norme est

4. NERC Implementation Plan, consulté le 8 octobre 2019 au https://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/2016-02_CIP_003-8_Implementation_Plan_Clean_04182019.pdf (en anglais seulement)
5. Ordonnance nº 843 de la FERC, consultée le 8 octobre 2019 au https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20No.%20743%20-%20Final%20Rule%20RM17-11-000.pdf (en anglais seulement).
6. Entente conclue conformément au décret n° 443-2019 du 8 avril 2019.

pertinente pour la fiabilité du réseau du Québec et qu'elle contribue à l'harmonisation avec les réseaux voisins.

3. ÉVALUATION PRÉLIMINAIRE DE L'IMPACT

Cette section présente l'évaluation préliminaire de l'impact selon le *coordonnateur de la fiabilité*.

CIP-008-6	Faible	Modéré	Important
Implantation de la norme	X		
Maintien de la norme	X		
Suivi de la conformité	X		

Légende :

Faible : Pratique normale de l'industrie ou norme n'entraînant que des ajustements mineurs aux processus ou aux pratiques en place.

Modéré : Changement qui nécessite de mobiliser certaines ressources matérielles, humaines ou financières pour implanter la norme proposée, la maintenir ou assurer le suivi de la conformité.

Important : Changement qui nécessite de prévoir et de mobiliser des ressources matérielles, humaines ou financières importantes pour planifier et implanter la norme proposée, la maintenir ou assurer le suivi de la conformité.

4. ÉVALUATION FINALE DE L'IMPACT

Les commentaires présentés dans le tableau ci-dessous ont été donnés par les entités lors de la consultation publique. Le Coordonnateur retranscrit d'une manière littérale les commentaires reçus.

Entité	Coûts de mise en œuvre	Coûts récurrents annuels	Justification
RTA	15 000 $	1 250 $	Mise à jour documentation, formation, procédures. Formation.
Total	**15 000 $**	**1 250 $**	

Projet QC-2019-05

Norme *CIP-008-6 – Cybersécurité – Sécurité physique des systèmes électroniques BES*

1. PRÉSENTATION DE LA NORME

1.1. Applicabilité de la norme

La norme CIP-008-6 s'applique aux fonctions visées suivants :

- *Exploitant d'installation de production* (*GOP*)
- *Propriétaire d'installation de production* (*GO*)
- *Responsable de l'équilibrage* (*BA*)
- *Coordonnateur de la fiabilité* (*RC*)
- *Exploitant de réseau de transport* (*TOP*)
- *Propriétaire d'installation de transport* (*TO*)
- *Certains distributeurs* (*DP*) [1]

Les *installations* visées sont :

- Les *installations* du *RTP* qui répondent aux critères définis dans la section Applicabilité.
- Certaines *installations* spécifiques des *distributeurs*.

1.2. Objet de la norme

L'objectif de la norme CIP-008-6 est de réduire les risques posés au fonctionnement fiable du *BES* par un *incident de cybersécurité* en définissant des exigences d'intervention en cas d'incident.

1.3. Contexte réglementaire

La Régie de l'énergie (ci-après, la « Régie ») a adopté la norme CIP-008-5 dans la décision D-2016-119[2] et la norme est en vigueur depuis le 1er janvier 2017.

La norme CIP-008-6 a été adoptée par le conseil d'administration de la NERC le 2 février 2019 et approuvée par la FERC le 20 juin 2019 dans le cadre du dossier RD19-3-000.[3]

[1] Voir la section Applicabilité des normes CIP pour les détails concernant l'application pour les distributeurs.
2. Régie de l'énergie, Décision D-2016-119, consultée le 13 août 2019 au http://publicsde.regie-energie.qc.ca/projets/335/DocPrj/R-3947-2015-A-0022-Dec-Dec-2016_07_29.pdf .
3. FERC, Docket No. RD19-3-000, consulté le 13 août 2019 au https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20Docket%20No.%20RD19-3-000.pdf (en anglais seulement)

1.4. Dispositions particulières pour le Québec

Le *Coordonnateur de la fiabilité* (ci-après appelé le « Coordonnateur ») propose de reconduire les spécificités québécoises, notamment le champ d'application et les dispositions particulières, déjà adoptées par la Régie dans sa décision D-2016-119 qui exempte certaines centrales et leur poste élévateur. La norme s'applique aux installations du *réseau de transport principal* (*RTP*) et aux installations spécifiées pour les *distributeurs*. De plus, les dispositions particulières suivantes s'appliquent

- Est exemptée de cette norme toute installation de production qui répond aux deux conditions suivantes : (1) la puissance nominale de l'*installation* est de 300 MVA ou moins et (2) aucun groupe de l'*installation* ne peut être synchronisé avec un réseau voisin.
- Sont exemptés de cette norme les postes élévateurs des *installations* de production exemptées selon le point précédent.

1.5. Dates d'entrée en vigueur proposées

La norme CIP-008-6 entrera en vigueur le 1er janvier 2021. Le plan de mise en œuvre aux États-Unis[4] précise que le délai entre l'approbation réglementaire et la mise en œuvre de la norme doit être de 18 mois.

Au Québec, le *C*oordonnateur propose le même délai de 18 mois entre l'adoption de la norme par la Régie et son entrée en vigueur.

1.6. Normes ou exigences à retirer

La norme CIP-008-5 doit être retirée dès l'entrée en vigueur de la norme CIP-008-6.

1.7. Modifications au Glossaire

Des modifications au Glossaire doivent prendre effet dès l'entrée en vigueur de la norme CIP-008-6. Les termes suivants sont modifiés :

- *incident de cybersécurité* ;
- *incident de cybersécurité à déclarer*.

Les définitions de ces termes sont présentées, en français et en anglais, dans le document *Modifications au Glossaire*.

Les définitions proposées au Glossaire dans le cadre du dossier R-4070-2018 pour les termes « automatismes de réseau » et « plan de défense » sont reconduites au Glossaire afin d'assurer que la norme NERC puisse faire l'objet d'une interprétation cohérente.

4. NERC Implementation Plan, consulté le 8 octobre 2019 au https://www.nerc.com/pa/Stand/Project%20201802%20Modifications%20to%20CIP008%20Cyber%20Secur/2018-02_CIP-008_Implementation%20Plan_Final%20Ballot_clean_01152019.pdf (en anglais seulement).

2. ÉVALUATION DE LA PERTINENCE

À la suite de l'ordonnance 848[5] de la FERC, la NERC a modifié la norme CIP-008-5 afin d'augmenter la notification obligatoire des *incidents de cybersécurité*, notamment les tentatives susceptibles de nuire au bon fonctionnement du *système de production-transport de l'électricité*.

La nouvelle norme CIP-008-6 ainsi que les modifications apportées aux définitions, aborde les quatre éléments décrits dans l'ordonnance 848 de la FERC[6] :

- le signalement d'*incidents de cybersécurité* compromettant ou tentant de compromettre un *périmètre de sécurité électronique* (*ESP*) (*Electric Security Perimeter*) ou un *système de contrôle ou de surveillance des accès électronique* (*EACMS*) (*Electronic Access Control or Monitoring System*) associé ;
- l'amélioration de la qualité des rapports d'*incidents de cybersécurité* en veillant à ce que chaque rapport comprenne des champs d'information spécifiés afin de faciliter la comparaison ;
- l'établissement des délais pour le dépôt des rapports d'*incident de cybersécurité* selon la gravité de l'incident ;
- l'obligation de transmettre les rapports de cybersécurité à l'Electricity Information Sharing and Analysis Center (E-ISAC) ainsi qu'au Department of Homeland Security (DHS) et à l'Industrial Control System Cyber Emergency Response Team (ICS-CERT).

En effet, les modifications quant à l'augmentation des types d'*incidents de cybersécurité* faisant l'objet d'une notification obligatoire, notamment les tentatives de compromettre un *ESP* ou un *EACMS* d'une entité ainsi que les révisions apportées aux exigences R1 à R4 tenant compte de l'ajout des EACMS associés aux *systèmes électroniques BES* à impact moyen et à impact élevé sont aussi pertinentes au Québec qu'ailleurs en Amérique du Nord.

Conformément à l'entente conclue en 2009 entre la Régie, la NERC et le NPCC et avec l'autorisation du gouvernement du Québec[7], cette norme a été élaborée et approuvée par des organismes externes pour l'Amérique du Nord, y compris le Québec. Le *coordonnateur de la fiabilité* est d'avis que cette norme est pertinente pour la fiabilité du réseau du Québec et qu'elle contribue à l'harmonisation avec les réseaux voisins.

3. ÉVALUATION PRÉLIMINAIRE DE L'IMPACT

Cette section présente l'évaluation préliminaire de l'impact selon le *coordonnateur de la fiabilité*.

5. Ordonnance nº 848 de la FERC, consultée le 8 octobre 2019 au https://www.ferc.gov/whats-new/comm-meet/2018/071918/E-1.pdf (en anglais seulement).
6. Consideration of Issues and Directives (en anglais seulement), consulté en ligne le 8 octobre 2019 au https://www.nerc.com/pa/Stand/Project%20201802%20Modifications%20to%20CIP008%20Cyber%20Secur/CIP-008_Consideration_of_Issues_and_Directives_Feb_2019.pdf (en anglais seulement).
7. Entente conclue conformément au décret n° 443-2019 du 8 avril 2019.

CIP-008-6	Faible	Modéré	Important
Implantation de la norme		X	
Maintien de la norme		X	
Suivi de la conformité		X	

Légende :

Faible : Pratique normale de l'industrie ou norme n'entraînant que des ajustements mineurs aux processus ou aux pratiques en place.

Modéré : Changement qui nécessite de mobiliser certaines ressources matérielles, humaines ou financières pour implanter la norme proposée, la maintenir ou assurer le suivi de la conformité.

Important : Changement qui nécessite de prévoir et de mobiliser des ressources matérielles, humaines ou financières importantes pour planifier et implanter la norme proposée, la maintenir ou assurer le suivi de la conformité.

4. ÉVALUATION FINALE DE L'IMPACT

Les commentaires présentés dans le tableau ci-dessous ont été donnés par les entités lors de la consultation publique. Le Coordonnateur retranscrit d'une manière littérale les commentaires reçus.

Entité	Coûts de mise en œuvre	Coûts récurrents annuels	Justification
RTA	15 000 $	1 250 $	Mise à jour documentation, formation, procédures. Formation.
HQT	20 000 $	30 000 $	Modifier l'ensemble des formulaires et processus liés à la déclaration d'incidents. Les coûts récurrents sont liés à une hausse potentielle du nombre de déclarations. Les coûts présentés sont un ordre de grandeur.
Total	**35 000 $**	**31 250 $**	

Projet QC-2019-05

Normes *CIP-005-6 – Cybersecurité- Périmètres de sécurité électronique*, *CIP-010-3 – Cybersecurité – Gestion des changements de configurations et analyses de vulnérabilité* et *CIP-013-1 – Gestion des risques de la chaîne d'approvisionnement*

1. PRÉSENTATION DES NORMES

1.1. Applicabilité des normes

Les normes CIP-005-6, CIP-010-3 et CIP-013-1 s'appliquent au même ensemble de fonctions visées et d'installations visées. Les fonctions visées sont les suivantes :

- *Exploitant d'installation de production* (*GOP*)
- *Propriétaire d'installation de production* (*GO*)
- *Responsable de l'équilibrage* (*BA*)
- *Responsable des échanges* (*IA*)
- *Coordonnateur de la fiabilité* (*RC*)
- *Exploitant de réseau de transport* (*TOP*)
- *Propriétaire d'installation de transport* (*TO*)
- Certains *distributeurs* (*DP*)

Les installations visées sont :

- Les *installations* du *RTP* qui répondent aux critères définis dans la section Applicabilité.
- Certaines *installations* spécifiques des *distributeurs*.

1.2. Objet des normes

Les exigences en matière de gestion de la chaîne d'approvisionnement visent à protéger les aspects de la chaîne d'approvisionnement qui relèvent de la volonté des entités responsables et s'appliquent aux *systèmes électroniques BES* à impact élevé ou moyen, conformément au processus d'inventaire et de catégorisation requis par la norme CIP-002-5.1a. Les chaînes d'approvisionnement pour les technologies de l'information et des communications ainsi que pour les systèmes de contrôle industriels présentent des risques pour le *BES* en permettant potentiellement l'introduction de menaces en matière de cybersécurité.

La nouvelle norme CIP-013-1 ainsi que les modifications apportées aux alinéas de la norme CIP-005-6 et de l'alinéa 1.6 de la norme CIP-010-3 imposent aux entités visées d'élaborer et de mettre en œuvre un plan abordant au moins quatre objectifs définis dans l'ordonnance n° 829 de la FERC :

- intégrité et authenticité des logiciels ;
- accès à distance par les fournisseurs ;
- planification des systèmes d'information ;
- gestion des risques liés aux fournisseurs et contrôles d'approvisionnement.

1.3. Contexte réglementaire

La Régie de l'énergie (ci-après, la « Régie ») a adopté la norme CIP-005-5 dans la décision D-2016-119[1] et la norme CIP-010-2 dans la décision D-2017-117[2]. Ces normes sont en vigueur depuis le 1er janvier 2017.et le 1er janvier 2018, respectivement.

Adoptées par le conseil d'administration de la NERC le 10 août 2017 et approuvées par la FERC le 28 octobre 2018 dans l'ordonnance n°°850[3], les normes CIP-005-6, CIP-010-3 et CIP-013-1 entreront en vigueur aux États-Unis le 1er juillet 2020.

1.4. Dispositions particulières pour le Québec

Le *Coordonnateur de la fiabilité* (ci-après appelé le « Coordonnateur ») propose de reconduire les spécificités québécoises, notamment le champ d'application et les dispositions particulières, déjà adoptées par la Régie dans sa décision D-2016-119 qui exempte certaines centrales et leur poste élévateur. La norme s'applique aux installations du *réseau de transport principal* (*RTP*) et aux installations spécifiées pour les *distributeurs*. De plus, les dispositions particulières suivantes s'appliquent

- Est exemptée de cette norme toute installation de production qui répond aux deux conditions suivantes : (1) la puissance nominale de l'*installation* est de 300 MVA ou moins et (2) aucun groupe de l'*installation* ne peut être synchronisé avec un réseau voisin.
- Sont exemptés de cette norme les postes élévateurs des *installations* de production exemptées selon le point précédent.

1.5. Dates d'entrée en vigueur proposées

Le plan de mise en œuvre aux États-Unis[4] précise que le délai entre l'approbation gouvernementale et la mise en œuvre des normes est de 18 mois. Les normes CIP-005-6, CIP-010-3 et CIP-013-1 enteront en vigueur le 1er juillet 2020. L'examen initial et l'approbation par le *cadre supérieur CIP* des plans de gestion des risques de la chaîne d'approvisionnement, selon l'exigence E3, doivent être terminés au plus tard à la date d'entrée en vigueur de la norme CIP-013-1.

Au Québec, le *C*oordonnateur propose le même délai de 18 mois entre l'adoption de la norme par la Régie et son entrée en vigueur.

1. Régie de l'énergie, Décision D-2016-119, consultée le 13 août 2019 au http://publicsde.regie-energie.qc.ca/projets/335/DocPrj/R-3947-2015-A-0022-Dec-Dec-2016_07_29.pdf.
2. Régie de l'énergie, Décision D-2017-117, consultée le 13 août 2019 au http://publicsde.regie-energie.qc.ca/projets/408/DocPrj/R-4005-2017-A-0009-Dec-Dec-2017_10_31.pdf.
3. FERC, Order No. 850, consultée le 13 août 2019 au https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20No.%20850%20Supply%20Chain%20Risk%20Management%20Reliability%20Standards.pdf (en anglais seulement).
4. NERC Implementation Plan, document consulté le 13 août 2019 au https://www.nerc.com/pa/Stand/Project%20201603%20Cyber%20Security%20Supply%20Chain%20Managem/Implementation_Plan_Clean_071117.pdf (en anglais seulement).

1.6. Normes ou exigences à retirer

Les normes CIP-005-5 et CIP-010-2 doivent être retirées dès l'entrée en vigueur des normes CIP-005-6 et CIP-010-3, respectivement.

1.7. Modifications au Glossaire

Les définitions proposées au Glossaire dans le cadre du dossier R-4070-2018 pour les termes « automatismes de réseau » et « plan de défense » sont reconduites au Glossaire afin d'assurer que la norme NERC puisse faire l'objet d'une interprétation cohérente.

2. ÉVALUATION DE LA PERTINENCE

À la suite de l'ordonnance 829[5] de la FERC, la NERC a élaboré une norme de fiabilité (CIP-013-1) qui traite de la gestion de la chaîne d'approvisionnement pour le matériel, les logiciels, les systèmes informatiques et les réseaux de systèmes de contrôle industriels ayant une incidence sur les opérations du *système de production-transport d'électricité* (*BES*). Les modifications à la norme CIP-005-5 répondent à la préoccupation de la FERC en ce qui concerne l'accès à distance par les fournisseurs. En ce qui concerne les révisions à la CIP-010-2, ils répondent à la préoccupation de la FERC associé à l'intégrité et là l'authenticité des logiciels. Ces modifications sont aussi pertinentes au Québec qu'ailleurs en Amérique du Nord.

Conformément à l'entente conclue en 2009 entre la Régie, la NERC et le NPCC et avec l'autorisation du gouvernement du Québec[6], cette norme a été élaborée et approuvée par des organismes externes pour l'Amérique du Nord, y compris le Québec. Le *coordonnateur de la fiabilité* est d'avis que ces normes sont pertinentes pour la fiabilité du réseau du Québec et qu'elles contribuent à l'harmonisation avec les réseaux voisins.

5. Ordonnance nº 829 de la FERC, consultée le 13 août 2019 au https://www.ferc.gov/whats-new/comm-meet/2016/072116/E-8.pdf (en anglais seulement).
6. Entente conclue conformément au décret nº 443-2019 du 8 avril 2019.

3. ÉVALUATION PRÉLIMINAIRE DE L'IMPACT

Cette section présente l'évaluation préliminaire de l'impact selon le *coordonnateur de la fiabilité*.

CIP-005-6	Faible	Modéré	Important
Implantation de la norme		X	
Maintien de la norme		X	
Suivi de la conformité		X	

CIP-010-3	Faible	Modéré	Important
Implantation de la norme		X	
Maintien de la norme		X	
Suivi de la conformité		X	

CIP-013-1	Faible	Modéré	Important
Implantation de la norme		X	
Maintien de la norme		X	
Suivi de la conformité		X	

Légende :

Faible : Pratique normale de l'industrie ou norme n'entraînant que des ajustements mineurs aux processus ou aux pratiques en place.

Modéré : Changement qui nécessite de mobiliser certaines ressources matérielles, humaines ou financières pour implanter la norme proposée, la maintenir ou assurer le suivi de la conformité.

Important : Changement qui nécessite de prévoir et de mobiliser des ressources matérielles, humaines ou financières importantes pour planifier et implanter la norme proposée, la maintenir ou assurer le suivi de la conformité.

4. ÉVALUATION FINALE DE L'IMPACT

Les commentaires présentés dans le tableau ci-dessous ont été donnés par les entités lors de la consultation publique. Le Coordonnateur retranscrit d'une manière littérale les commentaires reçus.

Entité	Coûts de mise en œuvre	Coûts récurrents annuels	Justification
CIP-005-6			
RTA	15 000 $	1 250 $	Mise à jour documentation, formation, procédures. Formation.
HQT	410 000 $	220 000 $	Documenter et définir les processus de gestion des accès fournisseurs aux actifs assujettis. Mise en place d'une solution de détection des communications suspectes. Les coûts présentés sont un ordre de grandeur.
CIP-010-3			
RTA	15 000 $	1 250 $	Mise à jour documentation, formation, procédures. Formation.

HQT	880 000 $	720 000 $	Mise en place des méthodes de vérification d'identité et d'intégrité des produits des fournisseurs et ajustement à la gestion des changements. Les coûts présentés sont un ordre de grandeur.
CIP-013-1			
RTA	50 000 $	5 000 $	Nouveau, intégration dans un processus RT existant, touche beaucoup de gens... Approbations à plusieurs niveaux Long délai d'implantation (18-24 mois)
HQT	700 000 $	350 000 $	Développement du plan de gestion de risque de la chaîne d'approvisionnement des composantes assujetties et mise en place des processus associés dans les différentes unités d'affaires touchées : majoritairement les Technologies de l'information, la Sécurité cybernétique, et l'Approvisionnement stratégique. Les coûts présentés sont un ordre de grandeur.
Total	**2 070 000 $**	**1 297 500 $**	