5 février 2018

**Agriculture ET AGROALIMENTAIRE Canada
Demande de renseignements SUR LA CYBERSÉCURITÉ 2017**

La Stratégie nationale et le plan d’action pour les infrastructures essentielles de Sécurité publique Canada établissent une approche de collaboration entre le gouvernement (fédéral, provincial, territorial) et le secteur de l’industrie pour atténuer l’ensemble des risques et menaces auxquels peuvent être exposés nos biens et systèmes essentiels. La chaîne d’approvisionnement alimentaire, dont les pêches, compte parmi les dix secteurs d’infrastructures essentielles désignés.

La Stratégie nationale tient compte du fait que les propriétaires et les exploitants d’infrastructures essentielles ont l’expertise et l’information dont les gouvernements ont besoin pour élaborer des plans de gestion des urgences détaillés et, qu’en retour, les gouvernements disposent de renseignements sur les risques et les menaces qui sont utiles aux propriétaires et exploitants dans le cadre de leurs activités de gestion des risques.

Ainsi, en collaboration avec la Coalition canadienne de la filière alimentaire pour la salubrité des aliments et la Coalition canadienne pour la santé des animaux, Agriculture et Agroalimentaire Canada (AAC) a préparé la présente demande de renseignements pour évaluer la sensibilisation actuelle à la question et obtenir de l’information sur des cybermenaces potentielles qui touchent le secteur de l’alimentation : comment elles peuvent apparaître et comment le secteur est prêt à y faire face. Cette demande aidera AAC à améliorer la préparation du secteur en fournissant les renseignements pertinents en temps opportun pour faciliter sa planification. Il aidera aussi le gouvernement du Canada à évaluer et à comprendre les menaces à la cybersécurité qui se posent actuellement dans le secteur.

Si vous avez des questions sur le sondage, y compris sur le contenu, l’objectif ou le format, ou si vous avez des commentaires, n’hésitez pas à écrire à AgEM-GUAg@AGR.GC.CA. AAC se servira de la rétroaction fournie pour orienter les efforts visant à améliorer les politiques, les programmes et les services à l’appui de la cybersécurité dans le secteur de l’alimentation.

**Date**:

**Nom de l’organisation :**

**Coordonnées**:

1. Cochez la case qui décrit le mieux votre organisation :

|  |  |
| --- | --- |
| [ ]  Association nationale | [ ]  Entreprise individuelle |

1. Cochez les cases qui décrivent le mieux le maillon auquel appartient votre organisation dans la chaîne d’approvisionnement :

|  |  |  |  |
| --- | --- | --- | --- |
| [ ]  | Production primaire | [ ]  | Importation |
| [ ]  | Transformation | [ ]  | Exportation |
| [ ]  | Fabrication | [ ]  | Autre (précisez) |
| [ ]  | Manutention et distribution | [ ]  | Commerce de détail |
| [ ]  | Entreposage | [ ]  | Services alimentaires |
| [ ]  | Transport |  |  |

1. Veuillez fournir les renseignements suivants concernant votre organisation :
* Nombre d’employés :
* Répartition géographique :
* Revenu annuel (facultatif) :

|  |
| --- |
| [ ]  0 $ - 500 000 $ |
| [ ]  500 000 $ - 1 000 000 $ |
| [ ]  1 000 000 $ - 5 000 000 $ |
| [ ]  5 000 000 $ - 10 000 000 $ |
| [ ]  10 000 000 $ - 50 000 000 $ |
| [ ]  Autre |

1. Cochez les cases qui décrivent le mieux la façon dont votre organisation assure la gestion de la technologie de l’information et le soutien connexe :

|  |  |
| --- | --- |
| [ ]  | Entièrement à l’interne (organisation dotée d’un effectif complet en TI et autonome)  |
| [ ]  | Gestion à l’interne (sous-traitance en TI – ordinateurs, services de réseaux, surveillance, développement d’applications et entretien)  |
| [ ]  | Partie du soutien à l’interne |
| [ ]  | Principalement ou complètement en sous-traitance  |

1. Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) de Sécurité publique Canada aide les organisations responsables d’infrastructures essentielles, les entreprises, les gouvernements provinciaux et territoriaux et les administrations municipales du Canada à protéger leurs systèmes informatiques. Il agit aussi comme ressource pour le signalement de cyberincidents et l’obtention de conseils sur la cybersécurité du gouvernement du Canada. Dans quelle mesure votre organisation connaît-elle le CCRIC?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| [ ]  **1** | [ ]  **2** | [ ]  **3** | [ ]  **4** | [ ]  **5** |
| Nous n’avons jamais entendu parler du CCRIC  | Nous en savons peu sur le CCRIC  | Nous connaissons plus ou moins le CCRIC | Nous connaissons l’existence du CCRIC, mais nous ne savons pas comment utiliser ses services  | Nous connaissons bien le CCRIC et nous avons déjà utilisé ses services  |

1. Différents types de cybermenaces peuvent peser sur les réseaux informatiques du secteur de l’agriculture, des pêches et de l’alimentation. Notons par exemple les réseaux de zombies, les tentatives de piratage, les intrusions de maliciels, l’hameçonnage, les attaques de rançongiciels, les pourriels et les virus. Votre organisation a-t-elle déjà connu une interruption ou une destruction de tout genre sur ses réseaux ou systèmes opérationnels (systèmes de contrôle) ou organisationnels au cours des deux dernières années?

|  |  |
| --- | --- |
| [ ]  Non | [ ]  Oui |

Il y a plus de deux ans?

|  |  |
| --- | --- |
| [ ]  Non | [ ]  Oui |

1. Si vous avez répondu Oui, veuillez préciser le type de cybermenaces et comment votre organisation est intervenue ou a atténué ces menaces.

*Réponse*

1. Comme il a été mentionné à la question 6, il existe différents cyberrisques pour les ordinateurs organisationnels et les ordinateurs et les dispositifs connectés à Internet qui, s’ils sont compromis, peuvent être altérés ou peuvent devenir des vecteurs qui altèrent d’autres parties de votre système. Plusieurs systèmes et dispositifs courants peuvent être visés, notamment les serveurs, les ordinateurs, les téléphones cellulaires et les appareils intelligents, les tablettes, les sites Web et les téléviseurs intelligents. Votre organisation a-t-elle des méthodes ou des protocoles en place pour protéger ces systèmes et dispositifs? Veuillez en dresser la liste.

|  |  |
| --- | --- |
| [ ]  |  |
| [ ]  |  |
| [ ]  |  |
| [ ]  |  |
| [ ]  |  |

1. Quels sont les types de renseignements que votre organisation a le plus intérêt à protéger pour éviter, en cas de compromission, des dommages financiers ou une atteinte à la réputation?

|  |  |
| --- | --- |
| [ ]  | Renseignements personnels des employés  |
| [ ]  | Renseignements sur les membres, les clients, les fournisseurs de services et de produits  |
| [ ]  | Propriété intellectuelle  |
| [ ]  | Données importantes sur les pratiques et les stratégies d’affaires |
| [ ]  | Autre (précisez)  |

1. Cochez les cases correspondant aux systèmes informatiques utilisés par votre organisation :

|  |  |
| --- | --- |
| [ ]  | Systèmes de contrôle de la production  |
| [ ]  | Systèmes de point de vente |
| [ ]  | Systèmes de géolocalisation par satellite  |
| [ ]  | Systèmes d’identification par radiofréquence  |
| [ ]  | Systèmes de données sur la traçabilité |
| [ ]  | Autre (précisez)  |

1. Êtes-vous satisfait de la capacité de votre organisation à détecter les cyberincidents et les cybermenaces, à y réagir et à en atténuer les risques?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| [ ]  **1** | [ ]  **2** | [ ]  **3** | [ ]  **4** | [ ]  **5** |
| Ne sais pas  | Non  | Un peu  | Oui, pour les petits incidents seulement  | Oui  |

1. Votre organisation offre-t-elle de la formation aux employés pour les sensibiliser à la sécurité physique?

|  |  |
| --- | --- |
| [ ]  Non | [ ]  Oui |

1. Votre organisation offre-t-elle de la formation aux employés pour les sensibiliser à la cybersécurité?

|  |  |
| --- | --- |
| [ ]  Non | [ ]  Oui |

1. Quel type d’information jugeriez-vous utile de recevoir de la part de spécialistes de la cybersécurité du gouvernement du Canada (comme le CCRIC) pour vous aider dans la planification et la préparation en cas de cyberattaques? Cochez toutes les réponses qui s’appliquent.

|  |  |
| --- | --- |
| [ ]  | Communiqués  |
| [ ]  | Séances d’information ciblées  |
| [ ]  | Formation  |
| [ ]  | Autre (précisez)  |

1. Comment votre organisation reçoit-elle actuellement de l’information sur les cybermenaces et les cyberincidents? Cochez toutes les réponses qui s’appliquent.

|  |  |
| --- | --- |
| [ ]  | Communiqués  |
| [ ]  | Séances d’information ciblées  |
| [ ]  | Formation  |
| [ ]  | Autre (précisez)  |

1. De qui votre organisation reçoit-elle actuellement de l’information sur les cybermenaces et les cyberincidents? Cochez toutes les réponses qui s’appliquent.

|  |  |
| --- | --- |
| [ ]  | Fournisseurs de services Internet  |
| [ ]  | Gouvernements  |
| [ ]  | Associations industrielles  |
| [ ]  | Fournisseurs de soutien technique  |
| [ ]  | Autre (précisez)  |

1. Votre organisation dispose-t-elle d’un plan de cybersécurité qui tient compte des piliers de la gestion des urgences, soit la prévention et l’atténuation, la préparation, l’intervention et le rétablissement?

|  |  |
| --- | --- |
| [ ]  Non | [ ]  Oui |

1. Utilisez-vous actuellement des pare-feu, des logiciels antivirus ou des services connexes pour protéger vos réseaux?

|  |  |
| --- | --- |
| [ ]  Non | [ ]  Oui |

1. Avez-vous des protocoles en place pour veiller à ce que les employés changent régulièrement leurs mots de passe?

|  |  |
| --- | --- |
| [ ]  Non | [ ]  Oui |

1. Dans quelle mesure votre organisation connaît-elle les normes ou les documents de cybersécurité ci-dessous?

**National Institute of Standards and Technology – Cadre sur la cybersécurité** (en anglais seulement)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ☐ **1** | ☐ **2** | ☐ **3** | ☐ **4** | ☐ **5** |
| Aucunement  | Très peu  | Plus ou moins  | Bien  | Très bien  |

**Organisation internationale de normalisation**

* **27001 – Systèmes de management de la sécurité de l’information**
* **27032 – Lignes directrices pour la cybersécurité** (en anglais seulement)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| [ ]  **1** | [ ]  **2** | [ ]  **3** | [ ]  **4** | [ ]  **5** |
| Aucunement  | Très peu  | Plus ou moins | Bien  | Très bien |

**Autres commentaires et suggestions**

N’hésitez pas à nous faire part de vos commentaires et suggestions.

*Réponse:*

Nous vous remercions de votre participation. Veuillez envoyer le questionnaire dûment rempli
au plus tard le **1 mars 2018** à l’adresse :

**AgEM-GUAg@AGR.GC.CA**

Pour signaler une cybermenace ou un cyberincident, vous pouvez communiquer en tout temps, sans frais, par courriel à ps.cyberincident-cyberincident.sp@canada.ca. Pour obtenir de plus amples renseignements sur la cybersécurité, consultez le site <https://www.securitepublique.gc.ca/ccric>.