Services de l'approvisionnement et des contrats
30, rue Victoria
Gatineau (Québec) K1A 0M6

MODIFICATION DE LA DEMANDE DE RENSEIGNEMENTS

Par la présente, la Demande de renseignements est modifiée; sauf indication contraire, toutes les autres modalités de la Demande de renseignements restent les mêmes.

N° de la modification :	**Date de la modification :**
2	Le 30 janvier 2018

Bureau du directeur général des élections – [N° du dossier] :

ECBR-RFI-17-0588

Titre :

Services de sécurité et de sécurité des TI

Date de clôture de la demande de renseignements:

Le 2 février 2018, à 14 h (HNE)

DEMANDES DE RENSEIGNEMENTS – Prière d'adresser toute demande de renseignements à l'autorité contractante:

Bureau du directeur général des élections
Services de l'approvisionnement et des contrats
30, rue Victoria
Gatineau (Québec) K1A 0M6

fournisseur@elections.ca

À l'attention de	**N° de tél.**
Barbara Robertson	819-939-1493

Partie 1. Interprétation

1.1 Élections Canada modifie par la présente et conformément à ce qui suit la demande de renseignements concernant le Services de sécurité et de sécurité des TI qui porte le numéro ECBR-RFI-17-0588 datée du 15 janvier 2018 (la « DR »). La présente modification fait partie intégrante de la DR.

1.2 Tous les mots et expressions définis dans la DR et employés dans la présente modification ont le sens qui leur a été donné dans la DR, à moins qu'ils ne soient définis autrement dans le présent document et sous réserve du contexte.

Partie 2. Questions et réponses

La question suivante a été posée suite à la DP et, par la présente, Élections Canada répond comme suit :

2.1 Question No. 1

Question : Dans le tableau des secteurs d'intérêt et des critères de l'annexe A, certains critères semblent ne pas correspondre aux secteurs d'intérêt. Ci-dessous se trouve le tableau original, suivi d'un autre tableau qui nous semble mieux adapté. Veuillez indiquer si notre interprétation est correcte.

Tableau original de la DR

Secteurs d'intérêt	**Critères**
Liste blanche et gestion des postes de travail	Devrait pouvoir empêcher l'exécution de tout logiciel non approuvé
	Devrait permettre de mettre à jour ou de modifier facilement la liste de logiciels approuvés
	Devrait permettre l'exécution d'applications dans un environnement de simulation/en isolation
	Devrait assurer des analyses de comportement pour détecter les maliciels potentiels
Détection des anomalies de trafic, enquêtes des systèmes informatiques et gestion des vulnérabilités	Devrait transmettre des avis par courriel et message texte
	Devrait permettre l'utilisation d'appareils mobiles comme source de notification
Systèmes de notification d'urgence	Devrait surveiller les activités inhabituelles dans l'infrastructure
	Devrait produire des alertes ou des avis d'activités suspectes
	Devrait permettre l'envoi de réponses automatisées
	Devrait permettre de bloquer les dispositifs de stockage de données non autorisés (c.-à-d., clés USB et DVD)

Prévention de la perte de données	Devrait permettre la visualisation du trafic
	Devrait signaler en temps réel les anomalies du trafic
	Devrait assurer des capacités d'enquêtes en ce qui a trait aux ordinateurs, aux serveurs et aux appareils mobiles
	Devrait fournir des outils pour maintenir l'intégrité de la preuve et de la chaîne de possession
	Devrait permettre l'identification des équipements réseaux et de découvrir les vulnérabilités
	Devrait fournir un catalogue des vulnérabilités découvertes et accorder la priorité à celles dont les niveaux de risque sont les plus élevés
	Devrait fournir des options ou de l'information sur la façon d'atténuer les vulnérabilités

Tableau modifié

Secteurs d'intérêt	**Critères**
Liste blanche et gestion des postes de travail	Devrait pouvoir empêcher l'exécution de tout logiciel non approuvé
	Devrait permettre de mettre à jour ou de modifier facilement la liste de logiciels approuvés
	Devrait permettre l'exécution d'applications dans un environnement de simulation/en isolation
	Devrait assurer des analyses de comportement pour détecter les maliciels potentiels
Systèmes de notification d'urgence ~~Détection des anomalies de trafic, enquêtes des systèmes informatiques et gestion des vulnérabilités~~	Devrait transmettre des avis par courriel et message texte
	Devrait permettre l'utilisation d'appareils mobiles comme source de notification
Prévention de la perte de données ~~Systèmes de notification d'urgence~~	Devrait surveiller les activités inhabituelles dans l'infrastructure
	Devrait produire des alertes ou des avis d'activités suspectes
	Devrait permettre l'envoi de réponses automatisées
	Devrait permettre de bloquer les dispositifs de stockage de données non autorisés (c.-à-d., clés USB et DVD)
	Devrait fournir des outils pour maintenir l'intégrité de la preuve et de la chaîne de possession
~~Prévention de la perte de données~~ Détection des anomalies de trafic, enquêtes des systèmes informatiques et	Devrait permettre la visualisation du trafic
	Devrait signaler en temps réel les anomalies du trafic
	Devrait assurer des capacités d'enquêtes en ce qui a trait aux ordinateurs, aux serveurs et aux appareils mobiles
	~~Devrait fournir des outils pour maintenir l'intégrité de la preuve et~~

gestion des vulnérabilités	~~de la chaîne de possession~~
	Devrait permettre l'identification des équipements réseaux et de découvrir les vulnérabilités
	Devrait fournir un catalogue des vulnérabilités découvertes et accorder la priorité à celles dont les niveaux de risque sont les plus élevés
	Devrait fournir des options ou de l'information sur la façon d'atténuer les vulnérabilités

Réponse : Élections Canada modifie, par la présente, le tableau qui se trouve à l'annexe A de la DR.

Dans le tableau, bon nombre des critères peuvent s'appliquer à différents secteurs d'intérêt. Le tableau modifié est une liste non exhaustive, qui présente les exigences minimales. Si un fournisseur ou sa solution peut répondre aux critères correspondant aux secteurs d'intérêt et aller au-delà de ces critères, Élections Canada aimerait obtenir cette information dans la réponse du fournisseur ou lors des présentations qui seront faites aux journées de consultation des fournisseurs. N'oubliez pas que les séances seront d'une durée limitée.

La DP est modifiée conformément à la section 3.2 de la présente modification.

Partie 3. Modifications

3.1 Modification de la date de clôture de la DR

La date de clôture de la demande de renseignements de la page couverture de la DR est modifiée à 14h00 (HAE) le 2 février 2018.

3.2 Modification de l'Annexe A de la DR

Par la présente, l'Annexe A de la DR est modifiée et doit être lue dans son intégralité comme suit :

ANNEXE A – SECTEURS D'INTÉRÊT EN SÉCURITÉ

PARTIE 1. Secteurs d'intérêt en sécurité

1.1. EC souhaite obtenir des renseignements de fournisseurs de l'industrie de la sécurité concernant des solutions possibles pour aider à préserver l'intégrité des élections à venir au Canada, plus particulièrement en ce qui a trait aux secteurs d'intérêt qui suivent.

1.2. Les critères indiqués pour chaque secteur d'intérêt présentent les fonctionnalités ou les capacités que le produit, le service ou la solution devrait comporter.

Secteurs d'intérêt	Critères
Liste blanche et gestion des postes de travail	Devrait pouvoir empêcher l'exécution de tout logiciel non approuvé
	Devrait permettre de mettre à jour ou de modifier facilement la liste de logiciels approuvés
	Devrait permettre l'exécution d'applications dans un environnement de simulation/en isolation
	Devrait assurer des analyses de comportement pour détecter les maliciels potentiels
Systèmes de notification d'urgence	Devrait transmettre des avis par courriel et message texte
	Devrait permettre l'utilisation d'appareils mobiles comme source de notification
Prévention de la perte de données	Devrait surveiller les activités inhabituelles dans l'infrastructure
	Devrait produire des alertes ou des avis d'activités suspectes
	Devrait permettre l'envoi de réponses automatisées
	Devrait permettre de bloquer les dispositifs de stockage de données non autorisés (c.-à-d., clés USB et DVD)
	Devrait fournir des outils pour maintenir l'intégrité de la preuve et de la chaîne de possession
Détection des anomalies de trafic, enquêtes des systèmes informatiques et gestion des vulnérabilités	Devrait surveiller les activités inhabituelles dans l'infrastructure
	Devrait permettre la visualisation du trafic
	Devrait signaler en temps réel les anomalies du trafic
	Devrait assurer des capacités d'enquêtes en ce qui a trait aux ordinateurs, aux serveurs et aux appareils mobiles
	Devrait fournir des outils pour maintenir l'intégrité de la preuve et de la chaîne de possession
	Devrait permettre l'identification des équipements réseaux et de découvrir les vulnérabilités
	Devrait fournir un catalogue des vulnérabilités découvertes et accorder la priorité à celles dont les niveaux de risque sont les plus élevés
	Devrait fournir des options ou de l'information sur la façon d'atténuer les vulnérabilités

	Devrait permettre l'exécution d'applications dans un environnement de simulation/en isolation

PARTIE 2. Exigences générales en matière de compatibilité

2.1 S'il y a lieu, le service, la solution ou le produit proposé devrait respecter les exigences suivantes :

a) le produit logiciel devrait être compatible avec Windows Server 2008, 2012, 2016 et Windows 7, 10;

b) le produit logiciel devrait être compatible avec Redhat Enterprise Linux;

c) les envois par courriel devrait être compatibles avec Microsoft Exchange Server;

d) l'authentification devrait être compatible avec AD/Kerberos;

e) la virtualisation devrait être compatible avec VMware;

f) le produit logiciel devrait pouvoir être intégré à un logiciel de gestion des informations et des événements de sécurité (GIES) commercial;

g) si un fournisseur offre un logiciel-service, toutes les données devraient demeurer au Canada.