Procurement and Contracting Services
30 Victoria Street
Gatineau, Quebec K1A 0M6

REQUEST FOR INFORMATION AMENDMENT

The Request for Information is hereby amended; unless otherwise indicated, all other terms and conditions of the Request for Information remain the same.

RFI Amendment No.	RFI Amendment Date:
2	January 30, 2018

Office of the Chief Electoral Officer File No.
ECBR-RFI-17-0588
Title:
Security and IT Security Services
Request for Information Closing Date:
February 2, 2018 at 2:00 p.m. EST

ENQUIRIES – address enquiries to the Contracting Authority:

Office of the Chief Electoral Officer of Canada
Procurement and Contracting Services
30 Victoria Street
Gatineau, Quebec K1A 0M6

supplier@elections.ca

Attention:	Tel No.
Barbara Robertson	819-939-1493

Part 1. Interpretation

1.1 Elections Canada hereby amends in accordance with this amendment the Request for Information for Security and IT Security Services bearing number ECBR-RFI-17-0588 and dated January 15, 2018 (the "RFI"). This amendment hereby forms part of the RFI.

1.2 Unless defined herein or unless the context otherwise requires, all of the words and phrases defined in the RFI and used in this amendment shall have the same meanings assigned to them in the RFI.

Part 2. Questions and Answers

The following question(s) have been asked in response to the Request for Proposal and Elections Canada hereby answers as follows:

2.1 Question No. 2

Question: In the table of Area of Interest and Criteria in Annex A it seems that some of the criteria may be misaligned with the area of interest. Below is the original and a second table that we think might reflect the actual intent. Please clarify if we are understanding this correctly.

Original in RFI

Area of Interest	**Criteria**
Whitelisting & EndPoint Management	Should have the ability to stop all unapproved software from running
	Should have the ability to easily update/modify the list of approved software
	Should allow application sandboxing/isolation
	Should provide behavioral analysis to detect potential malware
Anomalous Traffic Patterns, IT Forensics & Vulnerability Management	Should provide email and SMS notifications
	Should allow mobile devices as a notification source
Emergency Notification Systems	Should monitor unusual activity on infrastructure
	Should provide alerting/notification of suspicious activity
	Should provide automated response capability
	Should allow blocking of unauthorized data devices (i.e. USB Drives, DVDs)
Data Loss Prevention	Should provide visualizations of network data flows
	Should provide real-time alerting of traffic anomalies
	Should provide forensics capabilities for computers, servers and

	mobile devices
	Should provide tools to maintain evidence integrity and chain of custody
	Should provide automated scanning to identify assets and discover vulnerabilities
	Should provide a catalog of discovered vulnerabilities and prioritize those with the highest risk
	Should provide options or information on how to mitigate discovered vulnerabilities

Realigned

Area of Interest	**Criteria**
Whitelisting & EndPoint Management	Should have the ability to stop all unapproved software from running
	Should have the ability to easily update/modify the list of approved software
	Should allow application sandboxing/isolation
	Should provide behavioral analysis to detect potential malware
Emergency Notification Systems ~~Anomalous Traffic Patterns, IT Forensics & Vulnerability Management~~	Should provide email and SMS notifications
	Should allow mobile devices as a notification source
Data Loss Prevention ~~Emergency Notification Systems~~	Should monitor unusual activity on infrastructure
	Should provide alerting/notification of suspicious activity
	Should provide automated response capability
	Should allow blocking of unauthorized data devices (i.e. USB Drives, DVDs)
	Should provide tools to maintain evidence integrity and chain of custody
~~Data Loss Prevention~~ Anomalous Traffic Patterns, IT Forensics & Vulnerability Management	Should provide visualizations of network data flows
	Should provide real-time alerting of traffic anomalies
	Should provide forensics capabilities for computers, servers and mobile devices
	~~Should provide tools to maintain evidence integrity and chain of custody~~
	Should provide automated scanning to identify assets and discover vulnerabilities
	Should provide a catalog of discovered vulnerabilities and prioritize those with the highest risk
	Should provide options or information on how to mitigate discovered vulnerabilities

Answer: Elections Canada hereby modifies the table found in Annex A of the RFI.

In the table, many of the Criteria could be matched to many of the Areas of Interest. The modified table depicts a non-exhaustive list, as a minimum. If a supplier or their solution can meet the table's Areas of Interest and Criteria plus additional information, Elections Canada is interested in seeing this information in the supplier's response or at the Supplier Engagement Day presentations. Please remember that sessions will be time limited.

As such, the Request for Proposal is amended in accordance with 3.2 of this amendment.

Part 3. Amendments

3.1 Amendment to the RFI Closing Date

The Request for Information Closing Date on the cover page of the RFI is hereby amended to February 2, 2018 at 2:00pm (EDT).

3.2 Amendment to Annex A of the Request for Proposal

Annex A of the Request for Proposal is hereby amended to read in its entirety as follows:

ANNEX A – SECURITY AREAS OF INTEREST

PART 1. Security Areas of Interest

1.1. EC is seeking information from suppliers in the security industry about possible solutions to help preserve the integrity of future Canadian elections specifically related to the following Areas of Interest.

1.2. The Criteria listed for each Area of Interest identify the functionalities or abilities the product, service or solution should possess.

Area of Interest	Criteria
Whitelisting & EndPoint Management	Should have the ability to stop all unapproved software from running
	Should have the ability to easily update/modify the list of approved software
	Should allow application sandboxing/isolation

	Should provide behavioral analysis to detect potential malware
Emergency Notification Systems	Should provide email and SMS notifications
	Should allow mobile devices as a notification source
Data Loss Prevention	Should monitor unusual activity on infrastructure
	Should provide alerting/notification of suspicious activity
	Should provide automated response capability
	Should allow blocking of unauthorized data devices (i.e. USB Drives, DVDs)
	Should provide tools to maintain evidence integrity and chain of custody
Anomalous Traffic Patterns, IT Forensics & Vulnerability Management	Should monitor unusual activity on infrastructure
	Should provide visualizations of network data flows
	Should provide real-time alerting of traffic anomalies
	Should provide forensics capabilities for computers, servers and mobile devices
	Should provide tools to maintain evidence integrity and chain of custody
	Should provide automated scanning to identify assets and discover vulnerabilities
	Should provide a catalog of discovered vulnerabilities and prioritize those with the highest risk
	Should provide options or information on how to mitigate discovered vulnerabilities
	Should allow application sandboxing/isolation

PART 2. General Compatibility Requirements

2.1. Where applicable, the proposed product, service or solution should meet the following requirements:

a) Product software should work with windows Server 2008, 2012, 2016 and Windows 7, 10

b) Product software should work with Redhat Enterprise Linux

c) Email should work with Microsoft Exchange Server

d) Authentication should work with AD/Kerberos

e) Virtualization should work with VMware

f) Product software should be able to integrate with commercially available SIEM software

g) If a vendor is offering software as a service, all data should remain in Canada