Government of Canada Managed Security Service (GCMSS)

Annex A-5: Statement of Work - Antispam

Date: June 8, 2012

TABLE OF CONTENTS

REFERENCE

Please refer to Annex A - Appendix C: Definitions and Acronyms for a definition of terms and acronyms utilized throughout this annex.

1 ANTISPAM

(1) The Antispam is one of the GCMSS Threat Management Services. When ordered by Canada, by issuing a Task Authorization, the Antispam, as managed and implemented by the Contractor, must meet or exceed all of the requirements listed in this annex, in the balance of the SOW and elsewhere in the Contract prior to acceptance by Canada and during the entire period of the Contract.

1.1 Quality of Service

(2) The Antispam detection function must not exceed the rate of one false positive detection per million emails scanned. A false positive is the incorrect detection of spam in a legitimate email.

1.2 Detection and Response

(3) The Antispam must scan incoming and outgoing emails.

(4) The Antispam must detect spam emails.

(5) The Antispam must detect spam in email attachments including:

a) Microsoft Office;

b) PDF;

c) Image files; and

d) HTML.

(6) The Antispam must support multiple languages including double-byte character sets.

(7) The Antispam must have filtering systems that include but is not limited to:

a) regular expressions;

b) sender reputation scores;

c) sender IP reputation scores;

d) signature-based;

e) content-based;

f) message rate throttling;

g) Bayesian analysis;

h) message fingerprint analysis;

i) check-sum analysis;

j) heuristic evaluation;

k) message authenticity;

l) sender blacklists;

m) sender whitelists;

n) domain whitelists; and

o) domain blacklists.

(8) The Antispam must block fragmented messages.

(9) The Antispam must support email anti-spoofing including:

a) Message Sender Identification;

b) Sender Policy Framework;

c) SenderID;

d) Domain Keys Identified Mail; and

e) Reverse DNS check.

(10) The Antispam must offer a variety of responses including but not limited to:

a) Reject the email;

b) Discard the email; and

c) Accept the email with a warning message in the subject and message body as well as message header.

1.3 Message Handling

(11) The Antispam must support multiple email domains.

(12) The Antispam must support SMTP Mail Gateway for existing email servers specified by Canada.

(13) The Antispam must support LDAP-based email routing using an LDAP server specified by Canada.

(14) The Antispam must support SMTP Outbound Mail Relay.

1.4 Configuration

(15) When hosted under the GCMSS Threat Management Capacity, Feature Profile Type “XL”, the Antispam must:

a) provide inbound and outbound proxy Mail Transfer Agent (MTA) services, for email gateways specified by Canada, in support of DNS MX record redirect for content scanning and then relay email to its destination email server; and

b) support domain masquerading.

(16) The Antispam must support configuration of blacklists to allow customized entries by Client Organization.

(17) The Antispam must support configuration of whitelists to allow customized entries by Client Organization.

(18) The Antispam must support configuration of the sensitivity of the heuristic analysis by Client Organization.

1.5 Automatic Security Updates

(19) The Antispam must support automatic security updates of signatures and blacklists directly over the public Internet (i.e. no dependency of any intermediate device) at maximum every hour.

(20) The Contractor must provide automatic security updates within 15 minutes of availability from their supplier.

(21) The Antispam must apply security updates without rebooting within 15 minutes of receiving the updates.

1.6 Network Protocols

(22) The Antispam must monitor protocols including, but not limited to:

a) SMTP;

b) POP3; and

c) IMAP.

1.7 Reporting

1.7.1 Daily Reports

(23) The Contractor must provide a daily Antispam report to Canada in tabular and graphical format that includes:

a) a month to date incoming message activity summary in tabular format:

i) total incoming messages;

ii) number and percentage of messages stopped by reputation filtering;

iii) number and percentage of spam messages detected;

iv) number and percentage of virus messages detected;

v) number and percentage of threat messages detected; and

vi) number and percentage of clean messages accepted.

b) a month to date incoming message activity summary in pie-chart format:

i) number of stopped messages;

ii) number of spam messages detected;

iii) number of virus messages detected; and

iv) number of clean messages accepted.

c) a month to date incoming message activity summary in stacked column-chart format:

i) day of the month in the x axis; and

ii) total number of messages by type (stopped, clean, positive spam, suspected spam) stacked on the y axis.

d) a month to date tabular list of incoming messages per day with totals:

i) date;

ii) total incoming messages;

iii) total stopped messages;

iv) total positive spam messages;

v) total suspected spam messages;

vi) percentage of stopped messages;

vii) percentage of positive spam messages; and

viii) percentage of suspected spam messages.

e) a month to date tabular list of the top 7 recipient domains:

i) recipient domain;

ii) total incoming messages;

iii) total positive spam messages;

iv) percentage of positive spam messages;

v) total suspected spam messages; and

vi) percentage of suspected spam messages.

f) a month to date tabular list of the top 25 sender domains:

i) sender domain;

ii) total incoming messages;

iii) total positive spam messages;

iv) percentage of positive spam messages;

v) total suspected spam messages; and

vi) percentage of suspected spam messages.

g) a month to date outgoing message activity summary in stacked column-chart format:

i) day of the month in the x axis; and

ii) total number of messages by type (clean, positive spam, suspected spam) stacked on the y axis.

h) a month to date tabular list of outgoing messages per day with totals:

i) date;

ii) total outgoing messages;

iii) total positive spam messages;

iv) total suspected spam messages;

v) percentage of positive spam messages; and

vi) percentage of suspected spam messages.

1.8 Implementation

(24) The Contractor must inventory, review, optimize and implement in GCMSS existing rules, policies, and any other configuration of the existing Antispam solution of the Client Organization.

(25) The Contractor must document, review, optimize and implement in GCMSS configuration requirements of the Client Organization for the Antispam.

1.9 Change Management

(26) The Contractor must configure the response to positive spam detection, as specified by Canada, when requested by Canada within 2 FGWDs.

(27) The Contractor must configure sender blacklists, as requested by Canada, in accordance with priority levels as specified by Canada.

(28) The Contractor must configure domain blacklists, as requested by Canada, in accordance with priority levels as specified by Canada.

(29) The Contractor must configure sender whitelists, as requested by Canada, in accordance with priority levels as specified by Canada.

(30) The Contractor must configure domain whitelists, as requested by Canada, in accordance with priority levels as specified by Canada.

(31) The Contractor must configure the sensitivity of the heuristic analysis, as requested by Canada, in accordance with priority levels as specified by Canada.

(32) The Contractor must configure the Antispam MTA to correctly function with the DNS MX Record redirect, as requested by Canada, in accordance with priority levels as specified by Canada.