Government of Canada Managed Security Service (GCMSS)

Annex A-6: Statement of Work - Data Loss Prevention (DLP)

Date: July 12, 2012

TABLE OF CONTENTS

1 DATA LOSS PREVENTION (DLP) 1

1.1 DETECTION AND RESPONSE 1

1.2 DATA LOSS POLICY 2

1.3 END-POINT AGENT/SENSOR 3

1.4 CONFIGURATION 5

1.5 INTEGRATION 5

1.6 NETWORK PROTOCOLS 5

1.7 LOGGING 6

1.8 REPORTING 6

1.9 IMPLEMENTATION 9

1.10 MANAGEMENT SERVICES 9

REFERENCE

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

1 DATA LOSS PREVENTION (DLP)

(1) The Data Loss Prevention is one of the GCMSS Threat Management Services. When ordered by Canada, by issuing a Task Authorization, the DLP, 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 Detection and Response

(2) The DLP must block transmission of data based on Data Loss Policy in real-time.

(3) The DLP must scan outgoing packets.

(4) The DLP must scan SSL traffic.

(5) The DLP must scan inside encapsulated packets.

(6) The DLP must support full packet capture.

(7) The DLP must perform session reconstruction.

(8) The DLP must perform content analysis.

(9) The DLP must identify the service channel (mail, FTP, HTTP, etc.) based on packet content and not based on port number.

(10) The DLP must scan email traffic passing through MTA.

(11) The DLP must support multiple languages including double-byte character sets.

(12) The DLP must perform file cracking including:

a) scanning of over 100 file types;

b) scanning the following file types:

i) Microsoft Office 2003 (Access, Excel, OneNote, PowerPoint, Publisher, Word, Visio, Project) and above;

ii) Lotus Smart Suite version 9.7;

iii) Adobe PDF version 7 and above; and

iv) WinZip version 7 and above;

c) processing embedded files up to the bottom level.

(13) The DLP must decrypt the data or file if recovery keys are available.

(14) The DLP must respond to detected violations of the Data Loss Policy according to the response specified in the violated Data Loss Policy.

(15) The DLP must protect the confidentiality and the integrity of the Data Loss Policy violations.

(16) The DLP must support multiple distributed monitoring and enforcement points.

(17) The DLP must encrypt the data communicated between DLP nodes.

(18) The DLP fail safe state must be configurable to open or close as specified by Canada.

1.2 Data Loss Policy

(19) The DLP Data Loss Policy must include detection policies based on contextual factors including:

a) file signature (hash of the file);

b) file type;

c) encryption formats;

d) network protocols;

e) source IP address;

f) destination IP address;

g) sender email address;

h) recipient email address;

i) web services;

j) destination URL;

k) type of removable media utilized (USB, CD/DVD, diskette, PDA, phone, etc.);

l) removable device information, such as OEM, model number or serial number;

m) desktop applications utilized; and

n) all other contextual factors agreed to between the Contractor and Canada.

(20) The DLP Data Loss Policy must include detection policies based on content evaluation methods including:

a) rules-based/regular expressions;

b) data matching against authoritative sources identified by Canada;

c) partial document matching against authoritative sources identified by Canada for a complete or partial match to protected content;

d) statistical analysis based on machine learning, Bayesian analysis, and other statistical techniques;

e) lexicon analysis based on a combination of dictionaries, rules, and other conceptual analysis to protect loosely coupled information;

f) over 50 pre-built government-oriented categories with rules and dictionaries for common types of sensitive data including:

i) 16 digit numbers that meet credit card checksum requirements;

ii) 9 digit numbers that meet social insurance number checksum requirements; and

iii) other pre-built categories agreed to between the Contractor and Canada;

g) all other content evaluation methods agreed to between the Contractor and Canada.

(21) The DLP must include all other detection policies agreed to between the Contractor and Canada.

(22) The DLP Data Loss Policy must be enforceable for one or more of the following criteria:

a) all requests;

b) Client Organization;

c) enforcement or monitoring point;

d) the type of enforcement or monitoring point (network or End-Point);

e) destinations; and

f) channels/protocols.

(23) The DLP Data Loss Policy must include a configuration to:

a) select the action to take for violations including:

i) blocking transfer of the file;

ii) blocking transfer of the file and displaying a message;

iii) allowing transfer of the file but taking a snapshot of the file that will be attached to the incident record;

iv) allowing transfer of the file but encrypting the file using an encryption method specified by Canada; and

v) other actions agreed to between the Contractor and Canada;

b) select the action to take for violations based on:

i) the type of enforcement or monitoring point (network or End-Point);

ii) the target device;

iii) the target media;

iv) the sensitivity of the violation;

v) the severity of the violation; and

vi) the channel/protocol;

c) assign sensitivity and severity thresholds based upon volume of violations for the policy;

d) set a policy in test mode where violations of the Data Loss Policy are not reported as incidents but rather logged in a special test queue; and

e) set a policy in production mode where violations of the Data Loss Policy are logged as Incidents.

(24) The DLP must protect the confidentiality and the integrity of the Data Loss Policy.

1.3 End-Point Agent/Sensor

(25) The DLP End-Point Agent/Sensor must run on the following platforms:

a) MS Windows XP and above;

b) Red Hat Enterprise Linux Desktop 5.0 and above;

c) other operating systems as agreed to between Canada and the Contractor; and

d) the OEM dedicated hardware appliance.

(26) The DLP End-Point Agent/Sensor on OEM dedicated hardware appliance must:

a) support the Wire Speed of the Threat Management Capacity; and

b) be fully managed by the Contractor.

(27) The DLP End-Point Agent/Sensor must synchronize regularly, at a frequency specified by Canada, with the DLP central server to:

a) receive policy updates;

b) receive configuration updates;

c) receive software updates;

d) report new incidents; and

e) report status information.

(28) The DLP End-Point Agent/Sensor must apply Data Loss Policy configured for enforcement at the End-Point.

(29) The DLP End-Point Agent/Sensor must store Data Loss Policy violations locally, in a secure encrypted repository inaccessible to the user, until the violations can be reported to the DLP central server.

(30) The DLP End-Point Agent/Sensor must protect the End-Point in real-time based on the Data Loss Policy including:

a) preventing content from being written to portable or external media including:

i) USB enabled storage;

ii) CD/DVD/Diskette drives;

iii) smart devices; and

iv) unidentified LAN/PAN based storage.

b) automatic encryption of data being written to portable or external media;

c) preventing encrypted content from being written to portable or external media;

d) preventing content from being printed/faxed to unknown print/fax;

e) preventing content from being copied and pasted outside approved applications;

f) preventing content from being utilized with unapproved applications;

g) preventing screen capture;

h) preventing session recording;

i) disabling external devices outright; and

j) preventing content from being included in email and MIME attachments.

(31) The DLP End-Point Agent/Sensor must perform content analysis based on methods including:

a) rules/regular expressions;

b) partial document matching;

c) contextual analysis; and

d) other content analysis methods agreed to between the Contractor and Canada.

(32) The DLP End-Point Agent/Sensor must block transmission of data based on Data Loss

Policy in real-time.

(33) The DLP End-Point Agent/Sensor response to detected violations of the Data Loss Policy must include:

a) blocking transfer of the file;

b) allowing transfer of the file but requesting the user fills-in a justification form that will be attached to the incident record;

c) taking a snapshot of the transferred file that will be attached to the incident record; and

d) encrypting data copied onto a device.

(34) The DLP End-Point Agent/Sensor must selectively apply Data Loss Policy based on the network the End-Point is connected to.

(35) The DLP End-Point Agent/Sensor must provide performance controls including:

a) space quota allocation, specified by Canada, to store Data Loss Policy locally; and

b) space quota allocation, specified by Canada, to store incident information locally.

1.4 Configuration

(36) The DLP must allow the management and configuration of all aspects of Data Loss Policies.

1.5 Integration

(37) The Contractor must integrate the DLP with one or many web gateways specified by Canada using the ICAP protocol when requested by Canada within 5 FGWDs of a request at no additional cost to Canada.

(38) The Contractor must integrate the DLP with one or many reverse SSL proxy specified by Canada using the ICAP protocol when requested by Canada within 5 FGWDs of a request at no additional cost to Canada.

(39) The Contractor must integrate the DLP with one or many instant messaging IM proxy specified by Canada when requested by Canada within 5 FGWDs of a request at no additional cost to Canada.

1.6 Network Protocols

(40) The DLP must monitor protocols including:

a) TCP/IP;

b) ICMP;

c) FTP/FTPS;

d) UDP;

e) SMTP/SMTPS;

f) HTTP/HTTPS;

g) SIP;

h) SNMP;

i) DNS;

j) RPC;

k) NetBIOS;

l) Telnet;

m) SSH; and

n) all other protocols agreed to between the Contractor and Canada.

1.7 Logging

(41) The DLP must capture event data with appropriate metadata (date/time, user, protocol, etc.).

(42) The DLP must provide chain of custody support.

(43) The DLP must provide forensic data in a format compatible with third-party forensics tools.

(44) The DLP must log all violations of the Data Loss Policy, including at minimum:

a) failed policies along with actual values that caused the failure;

b) date and time;

c) source IP address;

d) destination IP address;

e) Client Organization;

f) detection or enforcement point;

g) network;

h) host;

i) application on host;

j) I/O channels (bus, Bluetooth, LPT, etc.);

k) external devices in use;

l) protocols; and

m) ports.

1.8 Reporting

1.8.1 Monthly Reports

(45) The Contractor must provide a monthly DLP End-Point aging report to Canada per Client Organization that includes:

a) number of End-Points configured;

b) number of End-Points that did synchronize with the DLP over the reporting month;

c) number of End-Points that did not did synchronize with the DLP over the reporting

month; and

d) a tabular list, by number of days descending, of the End-Points that did not did synchronize with the DLP over the reporting month:

i) End-Point identification;

ii) last synchronization date; and

iii) number of days since last synchronization.

(46) The Contractor must provide a monthly DLP management report to Canada per Client Organization that includes:

a) an executive summary comparing the number of events in the current month with the previous month, explaining in plain terms the differences and the drivers behind these statistics;

b) number of Incident Ticket of type “request for information” with pending status;

c) a problem management summary in tabular format;

i) Incident Ticket status (open, closed, pending); and

ii) Number of Incident Ticket;

d) number of Change Requests processed;

e) a list of Incident Ticket of Incident type “request for information” in tabular format;

i) date closed;

ii) date created;

iii) Ticket number;

iv) Incident severity;

v) Incident description;

vi) comments;

vii) Incident status;

viii) time to respond (in seconds); and

ix) time to contain (in seconds);

f) a list of Change Request Tickets in tabular format;

i) Ticket number;

ii) change description;

iii) comments; and

iv) status.

1.8.2 Daily Reports

(47) The Contractor must provide a daily DLP report by policy to Canada in tabular and graphical format by Client Organization that includes:

a) an event summary in bar-chart format for the top 5 policies;

i) total number of events for the policy on the x axis; and

ii) policy name on the y axis;

b) a top 50 event summary in tabular format;

i) policy;

ii) event detail;

iii) event severity; and

iv) number of events.

(48) The Contractor must provide a daily DLP report by severity to Canada in tabular and graphical format by Client Organization that includes:

a) an event summary, for the previous 2 weeks, in stacked column-chart format;

i) event date on the x axis; and

ii) total number of events by event severity stacked on the y axis;

b) an event summary, for the previous 2 weeks, in tabular format;

i) event date;

ii) event severity; and

iii) number of events.

(49) The Contractor must provide a daily DLP report by source IP to Canada in tabular and graphical format by Client Organization that includes:

a) an event summary in bar-chart format for the top 5 source IPs;

i) total number of events for the source IP on the x axis; and

ii) source IP on the y axis;

b) a top 50 event summary in tabular format;

i) source IP;

ii) event detail;

iii) event severity; and

iv) number of events.

(50) The Contractor must provide a daily DLP report by target IP to Canada in tabular and graphical format by Client Organization that includes:

a) an event summary in bar-chart format for the top 5 target IPs;

i) total number of events for the target IP on the x axis; and

ii) target IP on the y axis;

b) a top 50 event summary in tabular format;

i) target IP;

ii) event detail;

iii) event severity; and

iv) number of events.

1.8.3 Adhoc Report

(51) The Contractor must provide an adhoc report to Canada, based on severity as specified by Canada, of a Data Loss Policy violation that includes:

a) date and time of the violation;

b) channel involved;

c) the policy violated;

d) the specific content that triggered the incident;

e) the IP involved;

f) the criticality of the policy;

g) the severity of the incident;

h) a list of related incidents for the user;

i) a list of related incidents for the policy;

j) the full data content with the portion that triggered the incident highlighted;

k) the enforcement point; and

l) all metadata attached to the incident.

1.9 Implementation

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

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

1.10 Management Services

1.10.1 Change Management

(54) The Contractor must manage all aspects of Data Loss Policies, as requested by Canada, in accordance with priority levels as specified by Canada.

1.10.2 Incident Management

(55) The Contractor must log alerts from the DLP as Security Incidents.