Government of Canada Managed Security Service (GCMSS)

Annex A - Appendix C: Definitions and Acronyms

Date: July 12, 2012

1 DEFINITIONS

Term	Definition
Authentication	A process that establishes that a User has retained ownership or exerts control over the Credential that has been issued to them.
Authentication Service	A service that performs Authentication of a User.
Authority Revocation List	A list of revoked Certification Authority (CA) Certificates.
Availability Management	Process responsible for defining, analysing, planning, measuring and improving the availability of a service.
Canada excluding NCR	A site outside Canada NCR where GCMSS is implemented.
Canada NCR	A site within a radius of 100km from the Parliament of Canada where GCMSS is implemented.
Certificate	An electronic file, such as EPF or Entrust supported crypto-token, in a format which is in accordance with ITU-T recommendation X.509 V3 and which contains a public key of a subscriber, which can be an individual or a device, together with related information that is digitally signed with the private key of the Certification Authority that issued the Certificate.
Certificate Revocation List	A list issued and maintained by the Certification Authority of the Certificates that are revoked before their pre-set expiry time
Certification	Evaluation of the security features of an IT system and other related safeguards to establish the extent to which a particular design and implementation meets a specific set of security requirements, made in support of the accreditation process.
Certification Authority	An entity trusted by one or more entities to issue and manage X.509 public key certificates and CRLs. Each CA within the GC PKI may issue certificates under a choice of policies based on the level of assurance to which the CA has been accredited.
Change Management	Standardized methods and procedures that are used for handling all changes to an IT infrastructure/service to minimize the number and impact of any related incidents upon service.
Change Request	Request to make a change to the hardware, software, applications and processes used by the Contractor to deliver the GCMSS.
Change Ticket	A record of a Change Request.
Client Organization	A government organization that subscribes to the GCMSS to protect their network based on their own policies.
Configuration Item	Any component of an information technology infrastructure that is under the control of configuration management. CI can be individually managed and versioned, and they are usually treated as self-contained units for the purposes of identification and

Term	Definition
	change control.
Configuration Management	Standardized methods and procedures to control changes made to hardware and software components of a system throughout its lifecycle.
Credential	Unique physical or electronic identifier that is associated with an individual.
Cryptographic Module	The set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) and is contained within a cryptographic boundary (source: FIPS 140-2).
Denial-of-Service attack	An attempt to make a computer or network resource unavailable to its intended users.
Emergency Change	A Change Request to operationally restore a service where the failure or degradation of the service severely impacts service delivery or to correct a security Incident.
Federal Government Working Days	Monday to Friday excluding the following holidays as observed by Canada: New Year's Day Good Friday and Easter Monday Victoria Day St-Jean Baptiste Day (June 24th) Canada Day 1st Monday in August Labour Day Thanksgiving Day Remembrance Day Christmas Day Boxing Day
FIPS Mode	A mode of the Cryptographic Module that employs only approved security functions (not to be confused with a specific mode of an approved security function, e.g., Data Encryption Standard Cipher-Block Chaining (DES CBC) mode). This means that when a module is in the "FIPS mode", a non-FIPS approved method shall not be used in lieu of a FIPS-approved method. The FIPS 140-2 validation certificate will identify the cryptographic module's "FIPS mode" of operation (source: FIPS 140-2).
Firewall	Technology barrier designed to prevent unauthorized or unwanted communications between computer networks or hosts.
Firm Lot Monthly Price	Firm all-inclusive price per month for a specified number of units of an item.
Firm Monthly Rate	Firm all-inclusive rate per month.
Firm Unit Daily Rate	Firm all-inclusive unit rate per day.

Term	Definition
Firm Unit Hourly Rate	Firm all-inclusive unit rate per hour.
Firm Unit Monthly Rate	Firm all-inclusive unit rate per month.
Firm Unit Price	Firm all-inclusive one-time unit price of an item.
Firm Unit Rate per Minute	Firm all-inclusive unit rate per minute.
Host	Any IP addressable entity connected to an IP-based network.
Incident	An event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service.
Incident Management	Standardized methods and procedures to restore a service to normal operation as quickly as possible and to minimize the impact on business operations.
Information Security Operations Center	A location where Contractor owned and Contractor managed information systems (web sites, applications, databases, data centers and servers, networks, firewalls, desktops and other devices) are monitored, assessed, and defended. ISOC IT security staff monitors information systems for alarms and conditions to prevent, detect and manage cyber-attacks and other Security Incidents.
IP Host Resource Groups	A set of IP network resources.
Latency	Delays in packet transmission over a network between the point of ingress and the point of egress. The unit of latency is time, measured in milliseconds (ms).
Load Balancing	Process to share traffic between two or more IT resources (e.g. computers, network links, CPUs, hard drives etc.), in order to get optimal resource utilization, throughput, or response time.
Managed Service	Provision of a service to a Client where the supplier of the service has responsibility for delivery of the service and where the service must meet the Client's pre-defined service levels.
Management Services	Services provided by the Contractor that include: Change Management, Configuration Management, Incident Management, Release Management, Capacity Management and Availability Management.
Maximum Service Outage Time	Maximum accumulated outage time attributable to 1 or more Incidents in a calendar month.
Maximum Time to Restore Service	Maximum time to restore the GCMSS following an Incident resulting in an outage.
Most Popular Desktop Browser/Operating System Combinations	The top 95% of desktop browsers in use based on "MarketShare™ by Net Applications (http://marketshare.hitslink.com)" report Browser Share for Desktop demographics for North America.

Term	Definition
National Capital Region	As defined in SCHEDULE - DESCRIPTION OF NATIONAL CAPITAL REGION of the *National Capital Act* (http://laws-lois.justice.gc.ca/eng/acts/N-4/page-9.html#h-13).
Network Access Control	Policies for network access control that can include: pre-admission endpoint security policy checks; post-admission controls for users and devices on a network; and the access permissions of those users and devices.
Network Address Translation	The process of modifying IP address information in IP packet headers while in transit across a traffic routing device.
Personal Information	As defined in section 3 of the *Privacy Act* as, “information about an identifiable individual that is recorded in any form…”.
Privacy Breach	The result of an unauthorized access to, or collection, use or disclosure of Personal Information.
Privacy Impact Assessment	An assessment that describes the Personal Information flows in a project, and analyzes the possible privacy impacts that those flows might have.
Privacy Incident	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, and for an other than authorized purpose, have access or potential access to Personal Information in usable form, whether physical or electronic.
Regular Expression	Flexible means to match strings of text such as characters, words or patterns of characters.
Release Management	Standardized methods and procedures for the integration and flow of development, testing, deployment, and support of GCMSS services.
Secure Perimeter	A logical and physical boundary around Client network resources and information, which is controlled and protected against unauthorized access from outside of the boundary.
Security Breach	Unauthorized logical or physical access to an information system that has compromised the IT system’s confidentiality, integrity or availability.
Security Incident	An unauthorized behaviour (against the security policy of the IT system) regarding the operation and administration of the IT system that has the potential to compromise the IT systems confidentiality, integrity, or availability.
Security Requirements Traceability Matrix	A document used to ensure that all security requirements are included in the IT system and can be traced through the design, implementation and testing phases of the system development.
Security Testing	The processes to confirm that the technical security safeguards are functioning correctly.

Term	Definition
Security Validation	The process of establishing a correspondence, or mapping, between security requirements and the design elements or procedures that implement or address those security requirements.
Security Verification	The processes to confirm that proposed security safeguards and assurance requirements have been implemented correctly.
Service Delivery Point	A civic address where an instance of GCMSS is implemented.
Service Desk Response	Time required for the Contractor's Service Desk agent to answer a call.
Service Level	Value that is used to assess the performance, availability or quality of service, product or system.
Service Level Change Request Response	The Service Level for Change Request Response as described in GCMSS Annex A: SOW section Service Levels.
Service Level Maximum Service Outage Time	The Service Level for Maximum Service Outage Time as described in GCMSS Annex A: SOW section Service Levels.
Service Level Maximum Time to Restore Service	The Service Level for Maximum Time to Restore Service as described in GCMSS Annex A: SOW section Service Levels.
Service Level Response Time	The Service Level Response Time as described in GCMSS Annex A: SOW section Service Levels.
Service Level Service Desk Hold Time	The Service Level for Service Desk Hold Time as described in GCMSS Annex A: SOW section Service Levels.
Service Level Service Desk Response	The Service Level for Service Desk Response as described in GCMSS Annex A: SOW section Service Levels.
Service Level Service Portal Availability	The Service Level for the Service Portal Availability as described in GCMSS Annex A: SOW section Service Levels.
Service Level Task Authorization Response	The Service Level for Task Authorization Response as described in GCMSS Annex A: SOW section Service Levels.
Service Management Plan	Plan that specifies the Management Services to be provided by the Contractor for a GCMSS service.
Service Portal	Means the service portal provided and managed by the Contractor including the provision of documentation. The requirements are described in GCMSS Annex A: SOW subsection Service Portal.
SIEM Capacity	A single or a combination of physical or virtual devices which can run the SIEM service at an expected Transactions per Second (TPS).
Signature-based Intrusion Detection System	A system which can only detect attacks for which a signature has previously been created.
Software Maintenance Releases	All commercially available enhancements, extensions, improvements, upgrades, updates, releases, versions, renames,

Term	Definition
	rewrites, cross-grades, components and back grades or other modifications to the software for GCMSS developed or published by the Contractor or its licensor.
Software Support Maintenance Plan	Means the software support services provided and managed by the Contractor including documentation as described in Supplemental General Conditions 4004 (2010-08-16).
Statement of Sensitivity	Analysis of the sensitivity of the information processed, transmitted and stored using GCMSS.
Statistical Anomaly-based Intrusion Detection System	A system which, based on statistical anomalies, determines normal network activity like what sort of bandwidth is generally used, what protocols are used, what ports and devices generally connect to each other - and alert the administrator or user when traffic is detected which is anomalous (not normal).
Threat and Risk Assessment	A structured process designed to identify risks and provide recommendations for risk mitigation through analysis of system / service critical assets, potential threat events / scenarios, and inherent vulnerabilities.
Threat Management Capacity	A single or a combination of physical or virtual devices which can run concurrently all the Threat Management Services at an expected Wire Speed.
Threat Management Service	A security service, from the list below, that can be enabled on a Threat Management Capacity: • Firewall • Intrusion Detection & Prevention • Content Filtering • Anti-Virus • Anti-Spam • Data Loss Prevention
Upgrades	An update to the Licensed Software to add, extend, enhance and/or improve the existing features, functionality and/or performance of the program code, which is documented by a version or build number change to the right of the first decimal point (e.g., Product X Version 1.0 changes to Product X Version 1.1 or Product X Version 1.0.0 changes to Product X Version 1.0.1), regardless of whether the Contractor refers to it as a “minor upgrade” or “major upgrade”.
User	A person that uses the GCMSS.
User Device	An electronic device of a User that interact with GCMSS.
Virtual Local Area	Logical network partition for a LAN.

Term	Definition
Network	
Virtual Network	Logical network partition.
Virtual Route Forwarding	Technology that allows multiple instances of a routing table to co-exist within the same router at the same time.
VPN Tunnel	A connection for transmitting data securely through an unsecured network such as the Internet. A VPN is “virtual” because it does not require dedicated lines. It is “private” because encryption is used to achieve security.
Vulnerability Assessment	The processes to determine the existence of system vulnerabilities.
Warm Transfer	The service desk agent will remain on the line with the caller until the caller is transferred to their destination.
Web Based Training	Self-paced learning activities accessible via a computer or device with a web browser.
Wire Speed	When data is said to be transmitted at wire speed or at "wire rate," it implies there is little or no software overhead associated with the transmission and that the data travel at the maximum speed of the hardware.
Wireless Access Point	A device that allows wireless enabled Hosts to connect to a network using wireless network standards.

2 ACRONYMS

Acronym	Term
ARL	Authority Revocation List
BGP	Border Gateway Protocol
CA	Certification Authority
CAPV	Cryptographic Algorithm Validation Program
CBC	Cipher-Block Chaining
CD	Compact Disk
CI	Configuration Item
CMVP	Cryptographic Module Validation Program
CPU	Central Processing Unit
CRL	Certificate Revocation List
CSEC	Communications Security Establishment Canada
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DiffServ	Differentiated Services
DKIM	DomainKeys Identified Mail
DLP	Data Loss Prevention
DNS	Domain Name System
DoS	Denial of Service
DVD	Digital Video Disc
EAL	Evaluation Assurance Level
EIA	Electronic Industries Alliance
ERC	Enhanced Reliability Check
FGWD	Federal Government Working Days
FIPS	Federal Information Processing Standards
FOCIS	Fiber Optic Connector Intermateability Standard
FRTM	Functional Requirements Traceability Matrix
FTP	File Transfer Protocol
GC	Government of Canada

Acronym	Term
GCMSS	Government of Canada Managed Security Service
HIDS	Host-based Intrusion Detection System
HIPAA	Health Insurance Portability and Accountability Act
HTML	HyperText Markup Language
HTTP/HTTPS	Hypertext Transfer Protocol/ Hypertext Transfer Protocol Secure
ICAP	Internet Content Adaptation Protocol
ICMP	Internet Control Message Protocol
ICSA	International Computer Security Association
IDP	Intrusion Detection & Prevention
IDS	Intrusion Detection Service
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IM	Instant Messaging
IMAP	Internet Message Access Protocol
IP	Internet Protocol including IPv4 and IPv6
IPFIX	Internet Protocol Flow Information Export
IPS	Intrusion Prevention Service
IPsec	Internet Protocol Security
IRC	Internet Relay Chat
ISO	International Organisation for Standardization
ISOC	Information Security Operation Center
ISP	Internet Service Provider
IT	Information Technology
ITM	Integrated Threat Management
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEA	Log Export API
LMS	Learning Management System
LPT	Line Print Terminal or Local Print Terminal

Acronym	Term
MGCP	Media Gateway Control Protocol
MIME	Multipurpose Internet Mail Extensions
MPEG	Moving Picture Experts Group
MPLS	Multiprotocol Label Switching
MSS	Managed Security Services
MTA	Mail Transfer Agent
MTU	Maximum Transmission Unit
MX	Mail Exchanger
NAC	Network Access Control
NAT	Network Address Translation
NCR	National Capital Region
NIDS	Network-based Intrusion Detection System or Service
NIPS	Network-based Intrusion Prevention System or Service
OEM	Original Equipment Manufacturer
OPSEC	Open Platform for Security
ORP	Operational Readiness Plan
OS	Operating System
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PAN	Personal Area Network
PAT	Port Address Translation
PDA	Personal Digital Assistant
PDF	Portable Document Format
PIA	Privacy Impact Assessment
PKI	Public Key Infrastructure
PMP	Project Management Plan
POP3	Post Office Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RCA	Root Cause Analysis

Acronym	Term
RDEP	Remote Data Exchange Protocol
RFC	Request for Comments as per IETF
RIP	Routing Information Protocol
RPC	Remote Procedure Call
SCAP	Security Content Automation Protocol
SCCP	Skinny Call Control Protocol
SDEE	Security Device Event Exchange
SDP	Service Delivery Point
SIEM	Security Information and Event Management
SIM	Service Implementation Methodology
SIP	Session Initiation Protocol
SL-CRR	Service Level Change Request Response
SL-MSOT	Service Level Maximum Service Outage Time
SL-MTRS	Service Level Maximum Time to Restore Service
SL-RT	Service Level Response Time
SL-SDHT	Service Level Service Desk Hold Time
SL-SDR	Service Level Service Desk Response
SL-SPA	Service Level Service Portal Availability
SL-TAR	Service Level Task Authorization Response
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOW	Statement of Work
SRA	Secure Remote Access
SRTM	Security Requirements Traceability Matrix
SSC	Shared Services Canada
SSH	Secure Shell
SSL	Secure Sockets Layer
TA	Task Authorization
TACACS	Terminal Access Controller Access-Control System
TAP	Test Access Port
TBS	Treasury Board of Canada Secretariat

Acronym	Term
TCP	Transmission Control Protocol
TIA	Telecommunications Industry Association
TLS	Transport Layer Security
TPS	Transactions per second
TRA	Threat and Risk Assessment
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTM	Unified Threat Management
VLAN	Virtual Local Area Networks
VN	Virtual Network
VPN	Virtual Private Network
VRF	Virtual Route Forwarding
W3C	World Wide Web Consortium
WAP	Wireless Access Point
WBT	Web Based Training
WCAG	Web Content Accessibility Guidelines
WMI	Windows Management Instrumentation