Glossary of Terms

AAR - Activity Authorization Request - Proposal for [REDACTED] SIGINT development or collection related to [REDACTED] collection programs. Based on request and intelligence requirement from CFIOG, CSEC staff, or Second Party. [AGC0023 p 28]

Access - Refers specifically to raw data that is available to those within CSEC who are authorized to conduct or support

Acquire - Collect and intercept, used as synonyms for intercepted information. [AGC0186 p 30]

Active Monitoring - Monitoring of operational activities to assess compliance with policy instruments in effect, specifically related to legal compliance, and protection of privacy of Canadians. [AGC0118 p 64]

ANST - Active Network Security Testing - CSEC attempts to penetrate a client's computers or networks to look for vulnerabilities [AGC0132]

CANSLO - Canadian Special Liaison Officers [AGC0166]

CCIRC - Canadian Cyber Incident Response Centre – Unit under Public Safety [AGC0070]

CDO - Cyber Defence Operations - Operations under the IT Security mandate in the NDA regime [AGC0065]

CII - Canadian Identifying Information - Information that may be used to identify a Canadian person, organization, or corporation, including, but not limited to, names, phone numbers, email addresses, IP addresses, and passport numbers. [AGC0007]

CKB - Cyber Knowledge Bases - Location of retained data. Example: Malware Repository. [AGC0123]

CND - Computer Network Defence [AGC0111]

Collateral - Non-SIGINT information included in SIGINT reports because it contributes in some way to the SIGINT story [AGC0159 p 45]

Contact chaining - Looking at a targeted individual, then the people they contact, and the people they contact. MD defines contact chaining as a "method developed to enable the analysis, from information derived from metadata, of communications activities or patterns to build a profile of communications contacts of various foreign entities of interest in relation to the foreign intelligence priorities of the Government of Canada, including the number of contacts to or from these entities, the frequency of these contacts, the number of times contacts were attempted or made, the time period over which these contacts were attempted or made, as well as other activities aimed at mapping the communications of targeted foreign entities and their networks." [AGC0089 at p 44]

CFIOG - Canadian Forces Information Operations Group [AGC0023]

CPRI - Canadian Privacy Related Information [AGC0015]

CONOP - Concept of Operations [AGC0025]

CRO - Client Relations Officers - CSE officers who liaise with "clients" within Government of Canada and with Second Parties [AGC0110]

CTEC - Cyber Threat Evaluation Centre - Established late 2009 to build cyber defence capabilities, threat awareness, and strengthen defensive postures. [AGC006 5]

CTR - Common Traffic Repository - Consolidated database for DNI and fax traffic since 2009, and for DNR since 2010 [AGC0166, AGC0192 p 13]

CTSN - Canadian Top Secret Network - New name for MANDRAKE, CSE's secure online link with GC partners and for data storage [AGC0193 p 72]

CVE - Common Vulnerabilities & Exposures - Used in cyber defence to describe security vulnerabilities in computer systems that are exploited by hackers and other bad actors [AGC0106]

Data - For cyber defence activities, it is [REDACTED] obtained from computer systems or networks of importance to GC, including content and associated metadata [AGC0086]

DDI - Delivery Distribution Indicators - Used to permit automatic routing of reports to specific databases within SIGINT centres, especially NSA [AGC0206 p 163]

Detached Metadata - Metadata that bas been separated from associated data before being made available to a human, in cyber defence context [AGC0025]

DGA - Directorate General Access [AGC0193 p 20]

DGI - Directorate General Intelligence [AGC0193 p 20]

DGP - Directorate General SIGINT Programs [AGC0193 p 20]

DGPC - Director General, Policy and Communications - Has authority to approve inclusion of CII in Cyber Defence reports. [AGC0011]

Digraph - A two-letter code representing the location or nationality of a target entity. Each country has a two-letter digraph. A trigraph might contain the country and a code for the function of the targeted entity. [AGC0118]

DLS - Directorate of Legal Services [AGC0012]

DNI - Digital Network Intelligence - Internet-based data collection, such as email traffic or IP addresses.

DNR - Dialed Number Recognition - Phone or fax metadata, including calls to and from, date and time, and duration of calls.

DPSO - Data Provided By System Owner - Refers to information provided to CSE by the owners of third party electronic systems. [AGC0018]

D2 - See OPS.

ECI - Exceptionally Controlled Information - Sub- system of the COMINT control system that provides additional protection for very sensitive SIGINT operations. Details [REDACTED] [AGC0023]

ELINT - Electronic Intelligence [AGC0070]

EPR - End Product Reports [AGC0015]

FI - Foreign Intelligence.

FISINT – Foreign Instrument Signals Intelligence [AGC0182 p 109]

FLC – Foundational Learning Curriculum – A series of CSE training materials [AGC0240]

GCR – Government of Canada Requirement.

Framework for Addressing Risks in Sharing Information with Foreign Entities - Defines Canada's obligations for handling information with a risk of mistreatment or torture [AGC0080]

Identifiers - See Selectors.

Identifying Metadata - Metadata that could identify one or both communicants, or the communication itself. Identifying metadata is treated as private communication if it is retained. [AGC0122 at p 4]

IHS - Information Holding System - Responsible for the management and safeguard of the information created by CSE business lines and administration of CSEC Records Retention and Disposition Program [AGC0192]

IM - Information Management [AGC0192]

Integree - Someone seconded to CSE from a cryptologic partner org like NSA.

IPOC - IT Security Program Program Oversight & Compliance.

ISOM - Integrated SIGINT Operational Model – Governance structure for handling SIGINT [AGC0070]

ITSOI – CSEC IT Security Operational Instructions.

JRO - Joint Research Office [AGC0193 p 23]

LESA - Law enforcement and security agencies [AGC0193 p 29]

Liaison Officers - Second Party officers working in CSE facilities.

LIBRA - Steering group for recommendations following a shutdown of ITS cyber defence activities in 2006 [AGC0214 p 11]

MANDRAKE - Former name of the Canadian Top Secret Network, Secure government computer network with CSE reports [AGC0110, AGC0193 p 72]

Metadata First - The Metadata First initiative requires CSE to select communications traffic by running its programmed dictionary selectors at metadata (routing information) first (presumably before using it on content of intercepted private communications) [AGC0186 p 16]

MD - Ministerial Directive - Authorization from the Minister of National Defence allowing collection of metadata. Most recent in 2011.

Minimized - See Suppressed.

Mistreatment - Torture or other cruel, inhuman, or degrading treatment or punishment [AGC0080]

MOU - Memorandum of Understanding - Document setting out relationship between CSE and clients like CSIS [AGC0113 p 15]

MPER - Minor Procedural Errors Report [AGC0167]

MQT - Metadata Query Tool - CSE tool for querying metadata and conducting contact chaining (2010) [AGC0094]

MRA - Mistreatment Risk Assessment [AGC0168]

N Group - CSEC's Threat and Vulnerability Analysis Center in IT Security. [AGC0186 p 22]

Network Analysis and Prioritization - Used to identify and determine telecommunications links of interest derived from metadata. Involves acquisition of metadata, other [REDACTED] [AGC0004, AGC0023]

NSPL - National SIGINT Priorities List - GC priority list. Can be standing issues, which are long term interests, or watching briefs, which are short or medium term interest. [AGC0204 p 8]

OCS - Office of Cryptologic Studies [AGC0182]

OCT - Office of Counter-Terrorism [AGC0183]

OPS - Operational Policy Section - D2 - Department responsible for Operational Policy documents. Set of numbered guidebooks for operational policy - ie: OPS-X-X

PCs - Private Communications that originate or terminate in Canada and where the originator has a reasonable expectation of privacy [AGC0194 p 23]

Permutations - Format variations of an identifier within a given [REDACTED] [AGC0135]

PIF - Privacy Incidents File - Central record of privacy incidents "to track and demonstrate CSEC's commitment to protecting privacy, improve our own practices, ensure transparency, and enhance public confidence in CSEC" [AGC0011]

Privacy Incident - When the privacy of a Canadian is put at risk in a manner that runs counter to or is not provided for in CSE operational policies [AGC0167]

Querying - Searching or scanning raw data, automated or manual. [AGC0086]

Raw Data - Data that has not been determined to be relevant or essential, and has not been used or retained [AGC0122]

Report - Information prepared by CSEC which is approved for distribution outside CSEC and Second Party cyber defence counterparts. [AGC0124]

RFI - Requests for Information [AGC0113]

Second Parties - Five Eyes partners.

Secondee - Person temporarily moved from another Government of Canada entity or private organization to CSE, who then returns to their originating org [AGC0024]

Selectors - See Identifiers - Terms identifying a SIGINT target that can include a name, IP, email address, fax or phone number, or other characters, and are applied for the purpose of identifying traffic relating to foreign intelligence requirements and isolating it for processing. Selectors must be metadata. [AGC0007, AGC0118, AGC0186 p 15] Info used by network or service provider for routing purposes. Can include domain names. [AGC0086] Selectors subject to annual review. [AGC0118]

Selector Management - Process of managing selectors, including researching and developing new selectors, analysis of intercepted communications to confirm targeting is valid and productive, de-targeting selectors that are no longer productive [AGC0118 p 9]

Sharing - Data that has been used or retained, which may be made available to cyber defence counterparts within the Second Party community [AGC0123]

Signature - Automated queries that scan traffic or data for malicious cyber activity [ACG0080]

SIR - Standing Intelligence Requirement - [AGC0159 p 94]

SPI - SIGINT Programs Instruction - Materials to address policy gaps and grey areas, or info spread across policy documents. [AGC0087]

SPL - Security Product Line - CSIS reporting line for intelligence [AGC0113]

SPOC - SIGINT Programs Oversight and Compliance [AGC0019]

SPOR - SIGINT Programs Operational Requirements [AGC0182 p 17]

SSC - Shared Services Canada [AGC0070]

SSD - SIGINT Systems Development [AGC0182 p 71]

SSDPAC - SIGINT System Development Policy Awareness Course [AGC0210]

Substantial Risk of Mistreatment - A personal, present, and foreseeable risk of mistreatment. To be substantial, risk must be real and based on something more than mere theory or speculation. Test satisfied when it is more likely than not that there will be mistreatment. Test should not be applied rigidly, especially when the risk is of severe harm. [AGC0080]

Suppressed - See Minimized. “information excluded from SIGINT end-product or technical report because it may reveal the identity of a Canadian or Second Party entity. Stored in limited access database and replaced in report by generic terms.” [AGC0007]

TACREPs - Tactical Reports [AGC0157]

TAGs - Topic Area Guide - Alphabetic codes used to identify a report’s intelligence source [AGC0159 p 105]

Targeting - To single out for collection or interception purposes [AGC0118]

Technical Metadata - Metadata that does not identify either communicant. It is not treated as private communication and is not subject to retention requirements. Examples: Email protocol version, operating system, statistical information. [AGC0122 p 4]

Third Parties - Nations who are not Canada or Five Eyes partners.

Tippers - Time Sensitive Reports - Reports containing only enough information to allow for mitigation, and mitigation advice [AGC0124]

TIMC - Tuttle Institute for Mathematics and Computing - Classified mathematical and computational research institute within CSEC [AGC0182]

TKB - Target Knowledge Database [AGC0135]

Traffic - Content or payload of a communication or [REDACTED] plus the associated metadata acquired from the Global Information Infrastructure [AGC0007]

Triaging - Determining significance of data for purpose [AGC0025]

TSSA - Top Secret Special Access [AGC0182 p 182]

Unclassified Collateral – Information including radio and television broadcasts, wire service reports, newspapers, periodicals, reference works, public reports of government departments and agencies, and other information that has not been classified by a Canadian or Second Party government agency [AGC0159 p 53]