Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

TECHNOLOGY SUPPLY CHAIN GUIDELINES (TSCG)

CONTRACTING CLAUSES FOR TELECOMMUNICATIONS EQUIPMENT AND SERVICES

TSCG-01\G

October 2010

This page intentionally left blank.

Foreword

The *Contracting Clauses for Telecommunications Equipment and Services (TSCG-01|G)* is an unclassified publication, issued under the authority of the Chief, Communications Security Establishment Canada (CSEC).

Suggestions for amendments should be forwarded through departmental Information Technology Security (ITS) authorities to the ITS Client Services at CSEC.

For further information, please contact CSEC's ITS Client Services area by e-mail at itsclientservices@cse-cst.gc.ca or call 613 991-7654.

Effective Date

This publication takes effect on 10/15/2010

Originally signed by

Colleen D'Iorio
Acting Deputy Chief, IT Security

.

Table of Contents

List of Abbreviations and Acronyms

Acronym	Description
CC	Common Criteria
CISD	Canadian Industrial Security Directorate
CMVP	Crypto Module Validation Program
CSEC	Communications Security Establishment Canada
CSG	COTS Security Guidance
FSC	Facility Security Clearance
GC	Government of Canada
IPSec	Internet Protocol Security
ITS	Information Technology Security
NSE	National Security Exception
PWGSC	Public Works and Government Services Canada
RFP	Request for Proposal
SRCL	Security Requirements Checklist
TCP	Transmission Control Protocol
TRA	Threat and Risk Assessment
UPD	User Datagram Protocol

This page left intentionally blank.

1 Introduction

Several meetings involving an ad-hoc group of federal government departments occurred in April-May 2008 around an emerging national security issue relating to the vulnerability of the supply chain for Government of Canada telecommunications equipment and services.

In addition to the threat of cyber attack, there is a growing awareness of the risks posed by potentially vulnerable or shaped technologies that may be entering the Government of Canada (GC) communications networks and information technology infrastructure through the supply chain.

One way to reduce these risks is to include specific security clauses in PWGSC contracts that are aimed at protecting the integrity, availability and confidentiality of Canada's data and communications.

These clauses were developed based on a "managed telecommunications services" scenario, whereby a contractor is given responsibility for selecting, implementing, and operating and maintaining telecommunications infrastructure and services. It has been determined that the development of ideal or "one size fits all" security clauses is not feasible due to the evolving threats, and the variety and complexity of GC operational environments and resulting requirements.

2 Scope

These Guidelines describe a process for selecting and tailoring contract clauses to be incorporated in Public Works Government Services Canada (PWGSC) contracts with the objective of protecting the integrity, availability and confidentiality of Canada’s data and communications in managed services procurements. The objective of applying security clauses in these contracts is to prevent or to mitigate supply chain risks. Some of these clauses are also relevant for telecommunications solutions and equipment procurement.

These Guidelines should not be considered as an exhaustive list of possible clauses. Each requirement and the resulting contract clauses should be developed with specific threats and security requirements in mind. Selecting and tailoring clauses should also be done in conjunction with properly completing the Security Requirement Check List (SRCL) for contract and sub-contract requirements.

3 Trade-offs

As a part of selecting and applying these clauses in procurements, users should carefully consider the impact of the security measures that are selected on cost, schedule and operational requirements.

Clients should be looking for a reasonable trade-off between the increased cost of security requirements and the risk mitigation that would result from their use. PWGSC and CSEC can assist clients with these decisions, when requested. For further information on these guidelines, please contact CSEC Client Services.

4 Assumptions

There are three complimentary ways to address security issues in any given procurement:

1. By including mandatory or rated requirements in the evaluation criteria that screen out unqualified bidder technologies and solutions. For procurements covered by trade agreements, this means ensuring that the evaluation criteria are fully disclosed and comply with the trade agreements or determining that the National Security Exception (NSE) is appropriate and has been invoked;
2. By imposing contractual commitments on suppliers that provide some assurance of the integrity, availability and confidentiality of Canada's networks and data and mitigate the threats and vulnerabilities associated with potentially vulnerable or shaped technologies; and
3. By applying personnel, physical and operational security measures, for example the Crown can require the escort of contractors while on its premises.

This document addresses item (2) – contract clauses that can be selected and tailored for Public Works Government Services Canada (PWGSC) contracts. However, supply chain risk prevention or mitigation can also be enhanced through items (1) and (3).

5 Process

The selection and tailoring of the contracting clauses for incorporation in PWGSC contracts should follow the process described below.

1. There should be regular security briefings to PWGSC contracting officers by the appropriate security agencies. These briefings will help ensure that PWGSC contracting officers are kept aware of current threats and vulnerabilities and possible mitigation strategies; and

2. Upon receipt of a requisition for a telecommunications or network managed service, solution or major infrastructure procurement from a client department:

    a. The Contracting Officer offers to arrange, as required, a meeting between CSEC and/or other appropriate security agencies and the client department to discuss the requirements, including a review of the Industrial Security requirements identified in the SRCL and related threats;

    b. CSEC provides feedback to the client and PWGSC on supply chain (or other) security concerns (if any) associated with the planned procurement;

    c. If it is determined that additional security clauses are required to mitigate the threats, the Contracting Officer, working in collaboration with the CISD and CSEC, selects and tailors the appropriate security clauses;

    d. The Contracting Officer finalizes the security clauses and seeks a legal review with respect to:

        i. whether they are reasonably necessary to achieve Canada's security goals (and whether any of the clauses are inter-related – e.g., if one clause is deleted, is it important to keep another);

        ii. whether they are consistent with Canada's trade obligations (which will facilitate decisions about whether it is appropriate to invoke the NSE);

        iii. whether they are commercially reasonable (which may affect the quality and quantity of bids); and

        iv. whether they are consistent with CISD security obligations.

    e. This legal assessment will be discussed with CSEC and the client department and a final determination will be made on which clause(s), if any, to include in the contract.

6 Security Clauses

Each of the security clauses which follow is preceded by a description of the intent of the clause.

Note: Users are reminded that clauses should be tailored to address the specific requirements, and the specific threats and vulnerabilities associated with the requirement and planned procurement.

6.1 General Security Measures Surrounding Transmission of Sensitive Data

Objective: The following clause is intended to deal with concerns regarding the transmission of data, especially when the data is considered sensitive.

(a) The telecommunications [equipment/service] provided under the Contract will be used for the transmission of Government of Canada data of various kinds, including secure communications (at various security classification levels), privileged communications (such as Cabinet confidences and solicitor-client communications), and otherwise sensitive communications (including transmissions containing personal information of Canadians and proprietary or confidential information of third parties, such as suppliers). [Note to contracting officer: if the contractor will be collecting personal information and using it as part of the work, consider whether to include PWGSC Supplemental General Conditions 4008 (Personal Information).]

(b) The Contractor acknowledges that Canada requires, and the Contractor guarantees that, the telecommunications [equipment/service] provided under the Contract is and will be the subject of robust, comprehensive security measures that evolve as security threats and technologies evolve, so that the security measures in use are updated throughout the Contract Period, in order to achieve the highest possible levels of data integrity, availability, and confidentiality.

(c) The Contractor must implement any reasonable security or protection measures requested by Canada from time to time, within a reasonable timeframe agreed to with Canada. The parties agree that reasonableness will be determined based on the severity of the threat to the integrity, availability and confidentiality of Canada’s data and communications.

6.2 Security Clearance

Objective: The following clause is intended to identify requirements for security clearance of contractor personnel who have access to system facilities, equipment, or data. The level of clearance is dependent on the sensitivity level of the information and the criticality of the system. This requirement will need to be reflected in the SRCL and in the accompanying security guide for the procurement.

Security levels include:

Confidential - when compromise could reasonably be expected to **cause injury** to the national interest.

Secret - when compromise could reasonably be expected to **cause serious injury** to the national interest.

Top Secret - when compromise could reasonably be expected to **cause exceptionally grave injury** to the national interest.

With respect to the Article entitled "Security Requirement"

(a) The Contractor acknowledges that Canada may specify some equipment or networks as security sensitive and select a security classification in which case only security cleared employees and contractors may work on the system. Non-cleared persons may only assist in working on the system but not actually control or load software.

(b) Remote access to some systems may be permitted (Confidential and maybe Secret) but all keystrokes and uploaded software must be copied and kept as evidence for forensic purposes, if ever required.

(c) Upon arriving at Canada's premises, all Contractor and subcontractor personnel (which have been pre-approved by the Contracting Authority), must be able to provide proof of employment (such as a badge issued by the Contractor or the approved subcontractor) and their security clearance status must be ascertained from a trusted source;

(d) Individuals, although not having access to CLASSIFIED information or assets, may occupy positions that are deemed to be critical to the national interest. This includes personnel who have privileged access that give them the capability to effect major disruption or damage to critical systems. These individuals are to be security screened and granted a Security Clearance to a minimum of SECRET. Examples include technical or operational personnel, including network or system administrators or managers, who directly control the most sensitive and critical functionality such as monitoring, detection, back up and recovery information, testing and installation of security patches, configuration changes to security hardware and software, responding to security incidents etc.

NOTE: additional access controls are also required such as segregation of duties to assure that no individual has over-broad access to the most sensitive functionality. Secure audit records must be available to ensure such access may be auditably linked to a specific individual.

(e) The Contractor acknowledges that Canada may, at any time, refuse access to its premises to any individual. If that individual meets the security clearance requirements for the type of work being performed, but Canada refuses to provide any necessary access to that individual, any time described in the Contract for completing the portion of the Work to be performed by that individual will not start until Canada has informed the Contractor that access has been granted to that individual. Canada may advise the Contractor of the reason for denying access, but may also choose not to do so if Canada, in its discretion, has determined that there are security reasons for not disclosing the reason.

(f) The Contractor must obtain the required security clearance for all of its personnel before contract award. After contract award, it is the Contractor's sole responsibility to ensure that it has a sufficient complement of personnel to complete the Work who are cleared at the level required by the Contract.

(g) The Contractor acknowledges that Canada may revoke an individual's security clearance at any time.

6.3 Subcontracting

Objective: The following clause is intended to deal with situations where the Prime Contractor is not performing all of the work and there is a need to approve subcontractors for supply chain reasons.

Subcontracting:

(a) Despite the General Conditions, none of the Work may be subcontracted (even to an affiliate of the Contractor) unless the Contracting Authority has first consented in writing. In order to seek the Contracting Authority's consent, the Contractor must provide the following information:

(i) the name of the subcontractor;

(ii) the portion of the Work to be performed by the subcontractor;

(iii) the Designated Organization Screening or the Facility Security Clearance (FSC) level of the subcontractor as required by the work;

(iv) if requested, the security clearance status of individuals employed by the subcontractor who will require access to Canada facilities;

(v) completed sub-SRCL signed by the Contractor's Company Security Officer for CISD completion; and

(vi) any other information required by the Contracting Authority.

(b) For the purposes of this Article, a "subcontractor" does not include a supplier who deals with the Contractor at arm's length whose only role is to provide telecommunications equipment that will be used by the Contractor to provide services, including if the equipment will be installed in the backbone or infrastructure of the Contractor.

6.4 Network Diagram

Objective: The following clause applies to services or managed service contracts and is intended to deal with situations where there is concern as to the location of equipment in the network. The contractor would be required to provide information on the network layout being used to provide the services.

Network diagram:

(a) Within XX calendar days of Contract award, the Contractor must deliver a draft network diagram to the Technical Authority that, at a minimum, addresses the following:

(i) physical and logical network topology, depicting the nodes and connections amongst nodes in the network; and

(ii) details of the nodes in the network, protocols, bandwidths, etc.

(b) The Contractor must provide an updated network diagram to Canada at the end of the implementation period (if any) and then [weekly/monthly/quarterly], within 2 weeks of the end of each reporting period, which must reflect all changes made to the network during the reporting period. Even when there are no changes, the contractor is required to re-issue the Network Diagram with new dates at least [weekly/monthly/quarterly].

(c) The Contractor acknowledges that the network diagram is not proprietary to the Contractor.

6.5 Product Assurance and Equipment and Inventory

Objective: The following clause is intended to give Canada a complete list of equipment in use for delivery of the network services. The approach should be that, whenever possible, only Common Criteria (CC) certified and Crypto Module Validation Program (CMVP) validated products are trusted. The certification requirements should be listed in the mandatory evaluation criteria or in the specification. It should be noted that certification/validation requirements can impact the cost and time objectives of the planned procurement.

Equipment and Inventory:

(a) Within XX calendar days of Contract award, the Contractor must deliver a complete inventory of equipment deployed on Canada's network to the Technical Authority that, at a minimum, addresses the following:

- (i) Equipment owned by the Contractor;
- (ii) Equipment owned by Canada;
- (iii) Equipment owned by any third party (identifying that third party);
- (iv) The manufacturer of the equipment and country of origin;
- (v) The model and serial number of the equipment;
- (vi) Where each item of equipment is installed (reference to network diagram requirement describe in section 6.4 above);
- (vii) The date that the equipment was installed;
- (viii) The date on which the equipment was last serviced (whether for preventive or remedial maintenance);
- (ix) The date on which the Firmware was last updated.

(b) The equipment inventory must be integrated with the network diagrams required in section 6.4 above, so that, by reviewing the inventory, Canada can immediately locate on the network diagram where an individual item of equipment has been deployed within the network (and vice versa).

(c) The Contractor must provide an updated equipment inventory to Canada at the end of the implementation period (if any) and then [weekly/monthly/quarterly], within 2 weeks of the end of each reporting period, which must reflect all changes made to the network during the reporting period.

(d) The Contractor acknowledges that the equipment inventory is not proprietary to the Contractor.

(e) Before implementing the network services, the Contractor must provide the Technical Authority with a complete list of:

(i) the manufacturers (and any resellers, if the Contractor will not be purchasing the equipment directly from the manufacturer) of all equipment that it will deploy on Canada's network as part of the Work; and
(ii) the manufacturers (and any resellers, if the Contractor will not be purchasing the equipment directly from the manufacturer) of all equipment that it has or will deploy on its own or 3rd party network infrastructure or backbone that will be interconnected with Canada's network as part of the Work.

(f) At any time during the Contract, if the Contractor proposes to begin deploying equipment from a new manufacturer on Canada's network or on the Contractor's own or 3rd party infrastructure or backbone that will be interconnected with Canada's network, the Contractor must first obtain the written approval of the Technical Authority.

(g) The Contractor must not deploy any equipment on Canada's network or on its own or 3rd party network infrastructure or backbone that will be interconnected with Canada's network unless that equipment has been externally evaluated by a recognized certification body approved by Canada. (Note: a list of the recognized certification bodies that are recognized at the time of contract award or Request for Proposal (RFP) should be included in the RFP and subsequently in the contract.)

(h) At any time, if Canada notifies the Contractor that any given manufacturer is no longer considered a trusted manufacturer, the Contractor (and its subcontractors) must immediately cease deploying equipment made by that manufacturer in Canada's network and in any infrastructure or backbone of the Contractor that will interconnect with Canada's network. For already deployed equipment, the Contractor has to identify and/or remove equipment made by that manufacturer in Canada's network and in any infrastructure or backbone of the Contractor that will interconnect with Canada's network.

(i) If the Contractor becomes aware that any third party (other than a subcontractor) is deploying un-trusted equipment on its network, the Contractor must immediately notify the Technical Authority.

6.6 Location of Databases, Network Traffic Routing, and Data

Objective: The following clause is intended to ensure that Canada has control over the location of databases, network traffic and data, where there is concern with certain jurisdictions or the laws of a certain jurisdiction.

Location of Databases, Network Traffic Routing, and Data:

(a) The Contractor must ensure that all the databases containing any information related to the Work (including billing and/or call detail information) or data are located in Canada or, if the Contracting Authority has first consented in writing, to an alternate jurisdiction where:

(i) equivalent protections are afforded to personal information as in Canada under legislation such as the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* and under any applicable policies of the Government of Canada; and

(ii) the laws do not allow the government of that jurisdiction or any other entity or person to seek or obtain the right to view or copy any information relating to this Contract without first obtaining the written consent of the Contracting Authority.

(b) In connection with granting its consent to locating a database in a jurisdiction other than Canada, the Contracting Authority may require the Contractor to provide a legal opinion from a lawyer qualified in the foreign jurisdiction that the laws in that jurisdiction meet the above requirements, or may require the Contractor to pay for Canada to obtain such a legal opinion. Canada has the right to reject any request to house Canada's data in a jurisdiction other than Canada if there is a reasonable basis to be concerned about the confidentiality, availability, or integrity of Canada's data. Canada may also require that any data to be sent or processed outside of Canada be encrypted with Canada-approved cryptography and that the private key required to decrypt the data be kept in Canada in accordance with key management and storage processes approved by Canada.

(c) The Contractor must ensure that all databases on which any data relating to this Contract is stored/archived are physically and logically independent (meaning there is no direct or indirect connection of any kind) from all other databases, unless those databases are located in Canada (or in an alternate jurisdiction approved by the Contracting authority under paragraph (a) and otherwise meet the requirements of this Article.

(d) The Contractor must ensure that all data relating to this Contract is accessed and processed only in Canada or in an alternate jurisdiction approved by the Contracting Authority under paragraph (a).

(e) The Contractor must ensure that all domestic network traffic (meaning traffic initiated in one part of Canada to a destination or individual located in another part of Canada) is routed exclusively through Canada, unless the Contracting Authority has first consented in writing to an alternate route. The Contracting Authority will consider requests to route domestic traffic through an alternate jurisdiction that meets the requirements of paragraph (a).

6.7 Network Connectivity and Access Control

Objective: The following clause is intended to deal with authorized vs. unauthorized access to Canada's network(s) and database(s).

Network Connectivity and Access:

(a) The Contractor must safeguard the network and all databases including Canada's data or information about Canada at all times by taking all measures reasonably necessary to secure it and protect its integrity and confidentiality. To do so, at a minimum, the Contractor must:

(i) control access to all databases on which any data relating to this Contract is stored so that only individuals with the security clearance required by the Contract, and who also require access to the information in order to perform the Contract, are able to access the database;

(ii) ensure that passwords or other access controls are provided only to individuals who require access to perform the Work and who have the security clearance issued by CISD at the level required by the Contract; and

(iii) safeguard any database or computer system on which Canada's data is stored from external access using methods that are generally used, from time to time, by prudent public and private sector organizations in Canada in order to protect highly secure or sensitive information.

(b) Development, testing live or management networks must be segregated from each other and from Canada's existing networks.

(c) Unless requested by the Technical Authority, the Contractor must disable any TCP/UDP listening ports on any equipment deployed on Canada's network or on the Contractor's network infrastructure or backbone with which Canada's network is interconnected. Strong access control methods must be in place for all ports that are open for network management purposes.

(d) The Contractor must maintain an audit log that automatically records all attempts to access Canada's network, as well as any databases that include Canada's data or information maintained by the Contractor about Canada (such as billing information and call detail information). Every action, transaction or business function performed on the Contractor's network, systems, or databases relating to the Contract must be traceable to an individual user or account (by ensuring that user identifiers and accounts are unique and cannot be shared or transferred from one individual to another).

6.8 Network Management Protocols

Objective: The following clause is intended to deal with management of Canada's network(s). In collaboration with CSEC, more specific technical recommendations or baseline security requirements for remote access may be appropriate. The clause does not address specific safeguards, approaches, or techniques that could become obsolete during the contract period. As the network technology is changing rapidly, it is recommended that client departments contact CSEC for updates on security issues or threats to support requirements and procurement planning.

Network Management Protocols:

(a) The Contractor must ensure that [the equipment/all the components that form part of the system used to deliver the network services] can be managed using secure protocols.

(b) If the Contractor is using management servers that have a configurable level of security or encryption, the Contractor must disable all levels other than the highest level of security and/or encryption.

(c) The Contractor must not use protocols that send clear text usernames or passwords over the network.

(d) The Contractor must not use (and must disable any) protocols that cannot pass through session-aware firewalls.

(e) Canada will not consider an otherwise insecure protocol to be secure as a result of the use of tunnelling techniques such as port forwarding or Internet Protocol Security (IPSec).

(f) The Contractor must implement encryption protocols identified by Canada and must disable all encryption protocols not approved by Canada.

6.9 Vulnerability Assessment and Management

Objective: The following clause is intended to deal with vulnerability of equipment deployed in the network.

Vulnerability Assessment and Management:

(a) The Contractor must provide to the Technical Authority timely information about vulnerabilities (i.e., any weakness, or design deficiency, identified in [any equipment provided under the Contract/any component that forms part of the system used to deliver the network services) that would allow an unauthorized individual to compromise the integrity, confidentiality, access controls, availability, consistency or audit mechanism of the system or the data and applications it hosts.

(b) Where any vulnerability is caused by equipment manufactured by or software code written by the Contractor or one of its subcontractors, the Contractor must immediately remedy the vulnerability at its own cost.

(c) Where any vulnerability is caused by equipment manufactured by or software code written by a third party (other than a subcontractor), in addition to notifying the Technical Authority about the vulnerability as soon as the Contractor learns of it, the Contractor must implement any upgrades, patches or other fixes within a timeframe acceptable to Canada once they are made available by the manufacturer or software publisher, at the Contractor's own cost, unless the Technical Authority waives this requirement (in respect of a specific upgrade, patch or fix) in writing.

6.10 Resilience of Supply Chain and Disaster Recovery Plan

Objective: The following clause is intended to deal with business continuity and disaster recovery.

Resilience of Supply Chain and Disaster Recovery Plan:

(a) Within XX calendar days of Contract award, the Contractor must deliver a draft business continuity plan to the Technical Authority that, at a minimum, addresses the following:

(i) The steps the Contractor will take if any of its key suppliers go out of business;
(ii) The steps the Contractor will take if any of its key suppliers are identified as a supplier who no longer supplies "trusted" equipment; and
(iii) The steps the Contractor will take if any part of the network is harmed by any cause whether "natural" (Act of God) or malevolent.

The following paragraph outlines options for Canada if the supplier cannot guarantee availability of service due to a cyber-event or attack against the infrastructure of the supplier.

(b) The Contractor must address any concerns raised by Canada about the draft plan before finalizing the business continuity plan. Within 30 calendar days of each anniversary date of the Contract, the Contractor must provide the Technical Authority with an update to its business continuity plan.

(c) Within XX calendar days of Contract award, the Contractor must deliver a draft disaster recovery plan to the Technical Authority that, at a minimum, addresses the following:

(i) How frequently (no less than XX) all databases and systems will be backed up; and
(ii) How frequently (no less than XX) the Contractor's disaster recovery plan will be tested.

The Contractor must address any concerns raised by Canada about the draft plan before finalizing the disaster recovery plan. Within 30 calendar days of each anniversary date of the Contract, the Contractor must provide the Technical Authority with an update to its disaster recovery plan.

(d) Source Code Escrow Arrangement [for discussion based on the requirements and threats].

6.11 Physical Security

Objective: The following clause is intended to deal with physical security requirements applicable to Contractors premises in the use of service contracts.

Physical Security:

(a) The Contractor has to provide [select level of security] of physical security for [list component of the network].

6.12 Threat and Risk Assessment

Objective: The following clause is intended to deal with Threats and Risks that could compromise Canada's networks or the services being delivered by the Contractor. This clause would be in addition to the Threat and Risk Assessment (TRA) required for accreditation of a system.

Note: A requirement for the bidder to comply with ISO 27001/29100 or to provide deliverables such as "an assessment of supply chain risks" may be considered, though the cost and value of such measures should be carefully considered if the bidder in question is known by security agencies to be affiliated with un-trusted technologies.

Threat and Risk Assessment:

Within XX calendar days of the Contract being issued, the Contractor must submit to the Contracting Authority and CISD a threat and risk assessment, which must include:

(a) A list of all personnel to whom the Contractor has granted access to the network or to Canada's data, and the current level of security clearance granted to each individual by CISD;

(b) A description of all measures being taken by the Contractor (and, if applicable, its subcontractors) to protect its network infrastructure and backbone;

(c) A description of all measures being taken by the Contractor (and, if applicable, its subcontractors) to protect Canada's network;

(d) A description of all measures being taken by the Contractor (and, if applicable, its subcontractors) to protect Canada's data;

(e) A detailed explanation of any potential or actual threats to the network or any of Canada's data [delete if no access to Canada's data], together with an assessment of the risks created by these threats and the adequacy of existing safeguards to prevent these risks;

(f) An explanation of any new measures the Contractor intends to implement to safeguard the network and Canada's data; and

(g) Any information reasonably requested by the Technical Authority from time to time, including information required by the Technical Authority to perform its own threat and risk assessment in accordance with any applicable policies of the Government of Canada.

Within 30 calendar days of each anniversary date of the Contract, and at any time if requested by the Technical Authority, the Contractor must provide the Technical Authority with an update to its threat and risk assessment.

6.13 Security Monitoring and Incident Reporting

Objective: The following clause is intended to deal with abnormal and unauthorized use of the network.

Security Monitoring and Incident Reporting:

(a) The Contractor must monitor the network for abnormal or suspicious activities, such as odd work hours, unnecessary requests for code or data, abnormal data movements, or excessive use of systems or resources.

(b) The Contractor must immediately report to the Technical Authority and CISD any incidents relating to the security of Canada's network, or the Contractor's network infrastructure or backbone, or Canada's data, if it impacts Canada, including but not limited to those incidents listed in (a). For example, any unauthorized access or attempt to gain unauthorized access must immediately be reported. Also, the discovery of any virus or malicious code and/or the installation of any unauthorized software code on any equipment must immediately be reported.

(c) The Contractor agrees to cooperate fully with Canada in the investigation of any security incident.

6.14 Security Audit

Objective: The following clause is intended to allow Canada to audit the Contractor's compliance with the security requirements in service contracts.

Security Audit:

Canada may audit the Contractor's compliance with the security requirements included in the Contract at any time. If requested by the Contracting Authority, the Contractor must provide Canada (or Canada's authorized representative) with full access to its premises, its network, and all databases storing Canada's data or data related to the Contract at all reasonable times. If

Canada identifies any security deficiencies during an audit, the Contractor must immediately correct the deficiencies at its own expense.

6.15 Change in Control

Objective: The following clause is intended to require the Contractor to seek approval from Canada and CISD for a change in control. For the purposes of the General Conditions, the term “assignment” includes but is not limited to a change in control if the Contractor is a corporation, whether a direct or indirect change in the effective control of that corporation, whether resulting from a sale, encumbrances, or other disposition of the shares or by any other means. At present, PWGSC’s standard terms and conditions require consent for an assignment (which is required if the contractor sells its assets to another corporation who proposes to take over the performance of the contract), but no consent is required if another company is going to buy all the shares required for change of control. From a security perspective, it is expected that some contracts will require consent from Canada for a change in control.

In the case of a change of control, the Contractor must advise the Contracting Authority immediately. If Canada determines that the change of control poses a security risk to Canada, Canada reserves the right to terminate the contract for convenience.

7 Conclusion

The objective of applying these clauses in contracts is to prevent or to mitigate supply chain risks to Government of Canada telecommunications equipment and services. This document will be updated periodically based on lessons learned.