Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Contracting Clauses for Telecommunications Equipment and Services

Introduction There is 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.

What can be done? One way to reduce the risk of acquiring and deploying potentially vulnerable or shaped products is to include specific security clauses in Public Works Government Services Canada (PWGSC) contracts that are aimed at protecting the integrity, availability and confidentiality of Canada's data and communications. The objective of applying security clauses in contracts is to prevent or to mitigate supply chain risks to GC telecommunications equipment and services.

Security Clauses have been developed based on a "managed telecommunications services" scenario, whereby a contractor is given responsibility for selecting, implementing, operating and maintaining telecommunications infrastructure and services. Some of these clauses are also relevant for telecommunications solutions and equipment procurement.

Transmission of Sensitive Data – this clause addresses transmission of data, especially when considered sensitive;

Security Clearance and Escorting of Contractors – this clause addresses security clearances of Contractor personnel who have access to system facilities, equipment, or data;

Subcontracting – this clause addresses situations where the Contractor is not performing all of the work;

Network Diagram – this clause addresses services or managed service contracts where there is concern about the location of equipment in the network. The Contractor is required to provide information on the network layout being used to provide the services;

Product Assurance and Equipment and Inventory – this clause provides Canada with a complete list of equipment in use for delivery of the network service(s) and is complimentary to the Network Diagram clause;

Location of Databases, Network Traffic Routing and Data – this clause provides for Canada's control over the location of databases, network traffic and data;

Network Connectivity and Access Control – this clause addresses network and database access controls and logging of unauthorized access attempts;

Network Management Protocols – this clause addresses the use of secure communication and encryption protocols in GC networks;

Vulnerability Assessment and Management – this clause addresses the reporting and correction vulnerabilities discovered by the Contractor;

Supply Chain and Disaster Recovery Plan – this clause addresses Contractor planning and reporting on business continuity and disaster recovery requirements;

Physical Security – this clause addresses the physical security requirements applicable to the Contractor's premises to protect network infrastructure used in network or telecommunications service contracts;

Threat and Risk Assessment (TRA) – this clause requires the Contractor to conduct a TRA outlining the threats and risks that could compromise Canada's networks or the services being delivered by the Contractor;

Security Monitoring and Incident Reporting – this clause requires the Contractor to monitor and report on abnormal and unauthorized use of the network;

Security Audit – this clause permits Canada to audit the Contractor's compliance with the security requirements in service contracts; and

Change in Control – this clause requires the Contractor to seek approval from Canada for a change in effective control of the company that could occur through purchase of controlling interest.

Tailored for own Use Users should tailor the selected security clauses to address their specific requirements, and the threats and vulnerabilities associated with their planned procurement.

Trade-offs As a part of selecting and applying security clauses in procurements, users should carefully consider the impact of the security measures that are selected on cost, schedule and operational requirements. Users should be looking for a reasonable trade-off between the incremental cost of security requirements and the risk mitigation that would result from their use. PWGSC and Communications Security Establishment Canada (CSEC) can assist clients with these decisions, when requested. For further information on these guidelines, please contact CSEC Client Services.