Canadian Radio-television and Telecommunications Commission
Conseil de la radiodiffusion et des télécommunications canadiennes

REQUEST FOR PROPOSALS

CRTC FY 2017/18 RFP # 18-0001

OPERATOR OF THE NATIONAL DO NOT CALL LIST

APPENDIX E

INFORMATION TECHNOLOGY SECURITY REQUIREMENTS

Canada

1. INTRODUCTION

This document outlines the information technology (IT) security requirements for the Canadian Radio-television and Telecommunications Commission (CRTC) contract CRTC FY 2017/18 RFP # 18-0001 for the processing of sensitive data up to and including the level of Protected A. In absence of a formal Threat-Risk Assessment and due to the IT portion of the Security clearance being contract specific, the intent of this document is to state the minimum safeguards required in order that the processing of sensitive information be approved by the Department's IT Security Coordinator (ITSC):

Name: [Will be inserted when contract is awarded]
Information Technology Security Coordinator
Canadian Radio-television and Telecommunications Commission
Les Terrasses de la Chaudière, Central Building
1 Promenade du Portage
Ottawa, Ontario, Canada K1A 0N2
Tel: [Will be inserted when contract is awarded]
Email: [Will be inserted when contract is awarded]

Security is based upon layers of protection; that is, in order for the requirements of the IT Security (ITS) to effectively safeguard the information, they must be preceded and supported by other aspects of security and the associated policies. The physical, personnel and information security safeguards in accordance with the *Policy on Government Security* (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578) and ITS related Standards must exist prior to the implementation of ITS safeguards.

2. MANDATORY PREREQUISITES

2.1 Public Works and Government Services Validation for Physical Security

The application of the security safeguards listed in this document are based on the mandatory requirement that the physical premises have been inspected, certified and accredited to process and store sensitive information by the Canadian Industrial Security Directorate (CISD), Public Works and Government Services (PWGSC). The CRTC's Departmental Security Officer (DSO) will validate the certification and notify the IT Security Coordinator.

2.2 Security Policy Compliance Monitoring

The DSO's office will request a copy of the IT Security Inspection report, recommendations and vendor responses, when completed by the CISD.

The CRTC has the option to request the contractor to attend a Security/IT Security briefing session. In addition, on a frequency to be determined by the Safety, Security and Emergency Management Division (SSEMD), the CRTC retains the right to conduct inspections of the contractor's facility to ensure compliance with Government of Canada standards and policies with respect to the handling, storage and processing of protected/classified information.

3. MINIMUM IT SECURITY REQUIREMENTS

3.1 IT Security Policy Compliance and Monitoring

On a frequency to be determined by Technology Services Division/Information Technology Security, the CRTC retains the right to conduct inspections of the facility to ensure compliance with Government of Canada standards and policies with respect to prevention, detection, response and recovery requirements in the Operational Security Standard: Management of Information Technology Security (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328).

3.2 Storage, Disposal and Destruction of IT Media

All material such as CD/DVDs, flash/thumb drives, workstation hard disks, server hard disks, backup tapes and any other devices used to process or store protected information (including photocopiers, scanners and printers) must be retained and properly wiped or sanitized in a manner adhering to Government of Canada Communications Security Establishment ITSG-06: Clearing And Declassifying Electronic Data Storage Devices (https://www.cse-cst.gc.ca/en/publication/itsg-06) upon termination of the final contract.

In the event that equipment requires maintenance, support or replacement, no hardware associated with the processing or storage of protected or classified information may be given to an outside vendor.

3.3 Mobile Computing and Teleworking

Mobile computing and teleworking are prohibited. Laptops or any removable media, if used, containing protected/classified information may not be removed from the contractor's CISD-inspected site without the written approval of the DSO.

3.4 Minimum System/Software standards

All system and software components (i.e. Operating systems, Virtual Machines, Containers, Hypervisors, Server Hardware, Networking Hardware, system and software applications, firmwares, firewalls, etc.) must be updated on a regular basis to remediate security vulnerabilities and ensure system availability. Exact update scheduling is to be determined by the CRTC. The supplier must have current commercial support/maintenance contracts in place for the above mentioned component list. No component(s) of the solution must be at the “end-of-support” stage of its lifecycle during any point of the contract. End-of-support refers to a situation where the vendor/manufacturer of hardware, software application or operating system ceases to provide any of the following: technical assistance/support (online, phone or on-site), product updates, security patches or replacement parts for the product in question.

In addition, the following criteria must be enforced:

- No USB access to the associated system
- Printer access restricted to printing for financial tracking, reporting and record keeping purposes. Access Controls must be in place to prohibit the ability to print Consumer data collected by the system. Print jobs must be logged and retained for a minimum of 30 days.
- Implementation of a CAPTCHA for web requests
- Denial of service/Distributed Denial of Service protection against high traffic level (200Mbps link)
- Solution Zoning (Network Segmentation) diagram, to be reviewed and approved by the CRTC
- A valid Secure Sockets Layer (SSL) Certificate issued by a commercial Certificate Authority to enable encrypted communications through the use of Transport Layer Security (TLS) TLS/SSL, to be reviewed and approved by the CRTC

3.5 Incident Reporting

It is paramount that the CRTC's DSO and ITSC are made aware of any security-related incidents with respect to the facilities and equipment used to process and store sensitive information associated with CRTC's contracts.

The contractor must report any security-related incidents to the DSO and ITSC within two hours of an incident being detected or reported.

Name: [Will be inserted when contract is awarded]

Departmental Security Officer
Canadian Radio-television and Telecommunications Commission
Les Terrasses de la Chaudière, Central Building
1 Promenade du Portage
Ottawa, Ontario, Canada   K1A 0N2
Tel: [Will be inserted when contract is awarded]
Email: [Will be inserted when contract is awarded]