Public Works and Government Services Canada

Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:
Travaux publics et Services gouvernementaux Canada
Voir dans le document/
See herein
NA
Québec
NA

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

The referenced document is hereby revised; unless otherwise indicated, all other terms and conditions of the Solicitation remain the same.

Ce document est par la présente révisé; sauf indication contraire, les modalités de l'invitation demeurent les mêmes.

Comments - Commentaires
Document contient des exigences relatives à la sécurité

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Issuing Office - Bureau de distribution
Travaux publics et Services gouvernementaux Canada
Place Bonaventure, portail Sud-Oue
800, rue de La Gauchetière Ouest
7e étage, suite 7300
Montréal
Québec
H5A 1L6

Title - Sujet R&D Sécurité des systèmes embarqués	

Solicitation No. - N° de l'invitation W7701-227429/B	**Amendment No. - N° modif.** 001
Client Reference No. - N° de référence du client W7701-227429	**Date** 2022-02-09

GETS Reference No. - N° de référence de SEAG
PW-$MTB-255-16385

File No. - N° de dossier MTB-1-44036 (255)	**CCC No./N° CCC - FMS No./N° VME**

Solicitation Closes - L'invitation prend fin
at - à **02:00 PM** Eastern Standard Time EST
on - le **2022-03-03** Heure Normale du l'Est HNE

F.O.B. - F.A.B.
Plant-Usine: ☐ **Destination:** ☐ **Other-Autre:** ☐

Address Enquiries to: - Adresser toutes questions à: Desforges, Julie	**Buyer Id - Id de l'acheteur** mtb255
Telephone No. - N° de téléphone (514) 602-8307 ( )	**FAX No. - N° de FAX** ( ) -

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:

Instructions: See Herein

Instructions: Voir aux présentes

Delivery Required - Livraison exigée	**Delivery Offered - Livraison proposée**

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Telephone No. - N° de téléphone
Facsimile No. - N° de télécopieur

Name and title of person authorized to sign on behalf of Vendor/Firm (type or print)
Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)

Signature   **Date**

Canada

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7701-227429/B	001	MTB255
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
W7701-227429	MTB-1-44036	

MODIFICATION 001

The Request for proposal is modified as mentioned below:

1-Insert « Supplemental Security Classification Guide »
2-Correction of points to evaluation criteria (see points highlighted in yellow)

REPLACE Attachment 1 to Part 4 – Mandatory and Point Rated Technical Criteria

ATTACHMENT 1 TO PART 4 OF THIS BID SOLICITATION

MANDATORY AND POINT RATED TECHNICAL CRITERIA

1.   General

For each resource category, the Bidder must indicate the names of the proposed resources and should attach their résumés with all the evidences needed to show their education and experience (length in months at full time). Only the names proposed by the Bidder in each category will be evaluated for that category.

Below are examples of information allowing a complete evaluation of experience (applicable depending on the criterion):

- topic of the project or experience;
- nature of the project or experience;
- exact dates during which the project or experience was carried out (month and year of start and end);
- exact dates of the resource's involvement in the project (month and year of start and end);
- exact tasks carried out by the resource during the project or experience.

Only resources meeting the mandatory technical criteria will be assessed against the rated technical criteria. Resources that do not meet the mandatory technical criteria will not be part of the Contract, where applicable.

When the resources have been evaluated according to the mandatory technical criteria, the minimum resources required for the categories must be met by the Bidder. Failing this, the bid will be considered non responsive.

More than one resource may be proposed for a given category. In this case, each resource will be evaluated individually. Unless otherwise indicated, the overall scores obtained by each resource in the category in question will be added up and then divided by the number of proposed resources to obtain an average.

At Section 3- Point-rated criteria "Experience and expertise of resources", the final score will consist of the average score of the proposed resources of a given category. To be compliant, this score must be equal or higher than the requested minimum value. However, only the individual resources meeting the required minimum number of points for will be part of the Contract.

To be considered by the evaluation team, the diploma must be from a recognized Canadian university, or an equivalent established by a recognized Canadian credential-assessment service if the diploma or certificate was obtained abroad.
https://www.canada.ca/en/employment-social-development/programs/designated-schools.html

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7701-227429/B	001	MTB255
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
W7701-227429	MTB-1-44036	

Note 1: A Task Authorization may be considered as a project.

Note 2: The term embedded system used in the evaluation criteria is defined as a single device or a composition of devices that run almost exclusively on microcontrollers, Field Programmable Gate Arrays (FPGAs), digital signal processors or similar embedded processors. Also, embedded devices referenced in the evaluation criteria do not run or have a very small proportion of devices with an operating system (Windows; Linux, even in its embedded form, are operating systems). Consequently, a wireless router running a Linux operating system will not be considered as an embedded system for most specialist categories. Therefore, embedded system cyber security experience on such a device will not be considered as a valid for the cyber security of embedded system specialist. Experience on embedded device with operating systems will not be recognized for embedded system specialist and cyber security of embedded system specialist categories.

Note3: For the bidder to obtain points in part 3-Experience and Expertise of Resources of point-rated technical criteria, it should be demonstrated that the proposed resource has gained experience in one of the other areas of expertise listed below. The resource could also have a combination of experience including some of the areas of expertise listed.

2.   Mandatory Technical Criteria

General
2.1 For the categories of resources included into the Mandatory Technical Criteria, at least 13 different resources must be proposed by the Bidder, independently of the minimum number of people proposed per category. The Bidder must provide the list of the 13 resources and specify in which category (ies) they are proposed.
2.2 The same resource can be proposed for up to two categories and will therefore be assessed for each of those two categories. If the Bidder proposes a resource for more than two categories, the resource will only be evaluated for the first two categories selected in the order of appearance in the following table.
2.3 The proposed resources in each category must have the minimal education in the domain pertaining to the category or in related domain. If the proposed resource does not have a bachelor degree, a technologist diploma combined with three years of experience in the domain is acceptable. Those three years will be excluded from the experience in the Section 3. Experience and expertise of resource.
2.4 The Bidder must indicate in a table the names of the resource(s) to be evaluated for each category along with their degree. Categories with a minimum number of zero resource are optional.

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7701-227429/B	001	MTB255
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
W7701-227429	MTB-1-44036	

Category	Minimal education	Number and name of resources (minimum)
Project management	Bachelor degree	1
Programmer analyst	Bachelor degree	4
Electronics technologist	Technologist degree	1
Embedded system specialist - junior	Bachelor degree	2
Embedded system specialist - intermediate	Bachelor degree	2
Security of embedded system specialist	Bachelor degree	2
Traditional information technology (IT) security specialist	Bachelor degree	1
Software reverse engineer	Bachelor degree	No minimum (optional)
Wireless security specialist	Bachelor degree	No minimum (optional)
Laboratory technician	Technologist degree	No minimum (optional)
Hardware security of embedded systems specialist	Bachelor degree	No minimum (optional)

3. Point-rated technical criteria

SECTIONS	MIN. POINTS	MAX. POINTS
1. Technical proposal	18	40
2. Management model	8	20
3. Experience and expertise of resources	90	220
4. Experience of the bidder	-	15
5. Additional resources	-	24
6. Employment equities	-	15
TOTAL	116	334

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7701-227429/B	001	MTB255
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
W7701-227429	MTB-1-44036	

Table 1: Qualitative Criteria Evaluation Grid

Non-responsive	Extremely weak	Weak	Average	Superior	Exceptional
0 point	2 points	4 points	6 points	8 points	10 points
Did not submit information that could be evaluated	Does not meet requirements	Lacks details	Meets requirements	Exceeds requirements	Far exceeds requirements
	Weaknesses cannot be corrected	Weaknesses can be corrected	No significant weaknesses	No weaknesses identified	No weaknesses
	Unacceptable	Little chance of meeting performance requirements	Average capability, should be adequate for effective results	Superior capability, should deliver very effective results	Exceptional capability, should deliver extremely effective results

Table 2 – Point-rated criteria

DESCRIPTION	MIN. POINTS	MAX. POINTS
1. TECHNICAL PROPOSAL *Table 1 – Qualitative Criteria Evaluation Grid* will be used to assess the criteria.	18	40
1.1. Demonstrated understanding of scope and background Demonstrated understanding of the background and the scope should be complete and not limited to the description of each Task. The Bidder should use its own words to provide a convincing demonstration of its understanding.		10
1.2. Proposed technical approach and methodology The Bidder should clearly present its proposed technical approach and methodology to carry out the Work. The technical approach and methodology should be coherent, relevant, complete and realistic.		10
1.3. Risk element identification and management The Bidder should clearly describe all project components that could pose a risk and provide a plan for risk mitigation that would allow for the project's scope and the Tasks to be executed. The described components should be suitable and the mitigation plan realistic.		10
1.4. Clarity and accuracy of information provided The Bidder will be evaluated on the clarity and accuracy of the content of its proposal. The proposal should be well structured and easy to understand.		10
2. MANAGEMENT MODEL *Table 1 – Qualitative Criteria Evaluation Grid* will be used to assess the criteria.	8	20
2.1 Management methods and tools for planning, supervising and controlling tasks and activities		10

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7701-227429/B	001	MTB255
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
W7701-227429	MTB-1-44036	

The Bidder should outline the manner in which he/she proposes to oversee the management of Task Authorizations, and present the tools/techniques to be used for this purpose. The Bidder should address the following matters in his/her proposal: a. Proposed method for monitoring each task authorization (follow-up of the work progress according to proposed task authorization, budgetary follow-up); b. Approach to management given the unpredictable nature of a task authorization contract; and c. System put in place to ensure access to resources (provide at most two examples); if the use of business partners is provided for, agreements with these partners must be presented and signed by the partners in order to earn consideration.		
2.2 Quality assurance process The Bidder should describe its quality control process, which should, at a minimum, include: a. Verification and validation of work performed; b. Validation of compliance with the client's requirements; and c. Identification of future elements that could be improved. The Bidder should also demonstrate, using explanatory documents, that this method has been shown to be effective in previous projects.		10
3. EXPERIENCE AND EXPERTISE OF RESOURCES ***It is required that the Bidder obtained a minimum of 90 points overall for the technical evaluation criteria for that part. This required minimum is not the addition of required minimum for each criterion**.	**90**	**220**
3.1 Experience of proposed resources – Project management category	**3**	**10**
3.1.1 Experience in project management for research and development projects 10 points: at least 60 months of experience; 6 points: at least 48 months, but less than 60 months; 3 points: at least 24 months, but less than 48 months; 0 point: less than 24 months of experience		10
3.2 Experience and expertise of proposed resources – Programmer analyst category	**5**	**10**
3.2.1 Experience in software and architecture design, programming and debugging 3 points: at least 36 months; 2 points: at least 18 months, but less than 36 months; 1 points: at least 6 months, but less than 18 months; 0 point: less than 6 months.		3
3.2.2 – Expertise 3 points: at least 12 months of experience in Python programming 2 points: at least 12 months of experience in C, C++,Java or C# 2 points: at least 12 months of experience software and architectures design		7
3.3 Experience of proposed resources – Electronics technologist category	**3**	**10**

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7701-227429/B	001	MTB255
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
W7701-227429	MTB-1-44036	

3.3.1 Experience in fabrication, assembly, execution, test, installation or characterization of electronic or microelectronic components 10 points: at least 48 months of experience; 6 points: at least 36 months, but less than 48 months; 5 points: at least 24 months, but less than 36 months; 2 points: less than 24 months of experience.		10
3.4 Experience and expertise of proposed resources – Embedded system specialist category - Junior	**10**	**15**
3.4.1 Experience in design, test, characterization or integration of embedded systems. Experience in projects acquired in project-based courses or extra curriculum university projects is also considered. 5 points: at least 48 months; 4 points: at least 36 months, but less than 48 months; 3 points: at least 12 months, but less than 36 months; 1 point: less than 12 months.		5
3.4.2 Expertise 2 points: at least three university courses or equivalent project experience in embedded system design, tests, or integration 2 points: at least 6 months of experience with microcontroller programming or integration, JTAG (or equivalent), Inter-Integrated Circuit (I2C) or Serial Peripheral Interface Bus (SPI) 2 points: at least 1 month of experience with controller area network bus 2 points: at least 1 month of experience with field-programmable gate array (FPGA) 2 points: at least 2 months of experience with circuit board design, integration, test, characterization, fabrication, or assembly		10
3.5 Experience and expertise of proposed resources – Embedded system specialist category – Intermediate	**10**	**25**
3.5.1 Experience in design, test, characterization or integration of embedded systems 10 points: at least 144 months; 7 points: at least 96 months, but less than 144 months; 4 points: at least 48 months, but less than 96 months; 0 point: less than 48 months.		10
3.5.2 Expertise 5 points: at least 6 months of experience with controller area network bus 5 points: at least 12 months of experience with microcontroller programming, JTAG (or equivalent), Inter-Integrated Circuit (I2C) or Serial Peripheral Interface Bus (SPI) 5 points: at least 12 months of experience with circuit board design, integration, test, characterization, fabrication, or assembly		15
3.6 Experience and expertise of proposed resources – Security of embedded systems specialist category	**20**	**45**
3.6.1 Experience in characterization, penetration testing and identification and/or of mitigation solutions of embedded systems 5 points: at least 36 months; 3 points: at least 24 months, but less than 36 months; 2 points: at least 12 months, but less than 24 months; 0 point: less than 12 months.		5

3.6.2 Experience in characterization, penetration testing and identification and/or of mitigation solutions of automotive systems 15 points: at least 36 months; 10 points: at least 24 months, but less than 36 months; 5 points: at least 12 months, but less than 24 months; 0 point: less than 12 months.		15
3.6.3 – Expertise 5 points: at least 12 months of experience with security analysis of controller area network bus 4 points: at least 12 months of experience with security analysis of microcontroller firmware 4 points: at least 12 months of experience with fuzzing of embedded systems 4 points: at least 12 months of experience with characterization of embedded systems 4 points: at least 12 months of experience with Python programming 4 points: at least 12 months of experience with C programming		25
3.7 Experience and expertise of proposed resources – <u>Traditional IT security specialist category</u>	**10**	**25**
3.7.1 Experience in penetration testing 10 points: at least 60 months; 6 points: at least 36 months, but less than 60 months; 3 points: at least 12 months, but less than 36 months; 0 points: less than 12 months.		10
3.7.2 Expertise 5 points: at least 12 months of experience with vulnerability research, exploit and shellcode development on Unix systems (with memory corruption or buffer overflow) 5 points: Hands-on experience with penetration tools like Burp Suite, Wireshark, Metasploit, Nessus, Nmap or Scapy 5 points: having at least one of the following certifications: EC-Council Licensed Penetration Tester (LPT) Master, Certified Expert Penetration Tester (CEPT), Certified Red Team Operations Professional (CRTOP), Offensive Security Certified Professional (OSCP), Certified Ethical Hacker (CEH)		15
3.8 Experience and expertise of proposed resources – <u>Software reverse engineer category</u>	**10**	**20**
3.8.1 Experience in assembly code analysis and reversing 10 points: at least 36 months; 7 points: at least 18 months, but less than 36 months; 5 points: at least 6 months, but less than 18 months; 0 point: less than 6 months.		10
3.8.2 Experience in assembly code programming and debugging 5 points: at least 36 months; 3 points: at least 18 months, but less than 36 months; 2 points: at least 6 months, but less than 18 months; 0 point: less than 6 months		5

3.8.3 Expertise 2 points: experience developing plug-ins for IDA Pro and/or Ghidra 2 points: experience using IDA Pro and/or Ghidra 1 points: experience using other disassembler(s) (e.g., Binary Ninja, Capstone)		5
3.9 Experience and expertise of proposed resources – <u>Wireless security specialist category</u>	**8**	**20**
3.9.1 Experience in wireless security tests <mark>8 points</mark>: at least 48 months; 6 points: at least 24 months, but less than 48 months; 3 points: at least 12 months, but less than 24 months; 0 points: less than 12 months.		8
3.9.2 Expertise 4 points: at least 24 months of experience with security testing of wireless networks, including but not limited to Wi-Fi (802.11), Bluetooth (802.15.1), Zigbee (802.15.4), DECT, RFID, and cell networks 4 points: at least 12 months of experience with wireless testing tools like HackRF, LimeSDR and analysis software like gnu-radio, kismet, inspectrum 2 points: Offensive Security Wireless Professional (OSWP) certification 2 points: at least 12 months of experience with wireless network. It does not have to be security related.		12
3.10 Experience and expertise of proposed resources - <u>Laboratory technician</u>	**6**	**15**
3.10.1 Experience with advanced laboratory work, including electronics, chemistry, and physics laboratories 5 points: at least 48 months; 3 points: at least 24 months, but less than 48 months; 0 point: less than 24 months.		5
3.10.2 Expertise 5 points: at least 6 months of experience working with analysis methods with advanced equipment such as imaging technologies (digital or electronic microscope, x-rays), interferometers, and spectrometers 2 points: at least 6 months of experience working with bench-top test equipment such as oscilloscopes and logic analyzers, power supplies, or solder station 2 points: at least 2 months of experience working with a milling or computer numerical control machine 1 points: at least 2 months of experience in 3D printing or machining parts to build custom parts for test platforms		10
3.11 Experience and expertise of proposed resources - <u>Hardware security of embedded systems specialist</u>	**10**	**25**
3.11.1 Experience in hardware security of embedded system components such as developing tools for testing or conducting testing of embedded system hardware component security with techniques like fault injection, side-channel or semi-invasive analysis. 10 points: at least 36 months; 6 points: at least 24 months, but less than 36 months; 3 points: at least 12 months, but less than 24 months; 0 point: less than 12 months.	3	10

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7701-227429/B	001	MTB255
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
W7701-227429	MTB-1-44036	

3.11.2 Expertise 4 points: at least 12 months of experience with component hardware assurance or counterfeit detection 4 points: at least 12 months of experience with using fault injection techniques to detect if the system hardware implementation is protected against unauthorized access to data or secure enclave at the component level 4 points: at least 12 months of experience with analysing leaky side-channels in an embedded system to assess and validate hardware security at the component level 3 points: at least 12 months of experience with physical read out or probing techniques at the component level		15

DESCRIPTION	MIN. POINTS	MAX. POINTS
4 EXPERIENCE OF THE BIDDER The bidder should provide details about the projects in order to demonstrate that it meets the Bidder Experience criteria. To be considered, the project (or Task Authorization) must have been completed in the last ten years. A project can be considered for more than one of the following criteria.		**15**
4.1 Bidder's experience with R&D projects (worth at least $100,000, excluding taxes) 5 points: The Bidder (company) has completed at least 5 R&D projects. 3 points: The Bidder (company) has completed 3 or 4 R&D projects. 0 point: The Bidder (company) has completed fewer than 3 R&D projects.		5
4.2 Bidder's experience with embedded system security projects (worth at least $100,000, excluding taxes) 5 points: The Bidder (company) has completed at least 3 embedded system security projects. 3 points: The Bidder (company) has completed 1 or 2 security of embedded system projects. 0 point: The Bidder (company) has not completed any security of embedded system projects.		5
4.3 Bidder's experience with military system projects (platforms, sensors, and weapon systems) (worth at least $100,000, excluding taxes) 5 points: The Bidder (company) has completed at least 4 military system projects. 3 points: The Bidder (company) has completed 1 to 3 military system projects. 0 point: The Bidder (company) has not completed any military system projects.		5

DESCRIPTION	MIN. POINTS	MAX. POINTS
5. ADDITIONAL RESOURCES		**24**
5.1 The Bidder has proposed at least one additional resource beyond the minimum required by the mandatory criteria for the Cyber security traditional information system specialist (Section 3.7).		12
5.2 The Bidder has proposed at least one additional resource beyond the minimum required by the mandatory criteria for the Software revere engineering category (Section 3.8).		12

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7701-227429/B	001	MTB255
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
W7701-227429	MTB-1-44036	

DESCRIPTION	MIN. POINTS	MAX. POINTS
6. EMPLOYMENT EQUITY		**15**
6.1 The bidder proposes resource designated by the Employment Equity Act (https://www.canada.ca/en/employment-social-development/corporate/portfolio/labour/programs/employment-equity/federal-contractors.html). To be considered, these resources must be part of one or many of the following groups: women, indigenous peoples, persons with disabilities and members of visible minorities. Bidder must identify the resource and the groups. **Score is 5 points per resource that qualifies, for up to three resources.**		15

ALL OTHER TERMS, CLAUSES AND CONDITIONS REMAIN UNCHANGED

Security Requirement Checklist (SRCL)
Supplemental Security Classification Guide

This form must be completed in addition to SRCL question 7.b) <u>when multiple release restrictions</u> are therein identified <u>and/or</u> in addition to SRCL question 10.a) <u>when multiple levels of personnel screening</u> are therein identified.

Part A - Multiple Release Restrictions: Security Classification Guide

To be completed in addition to SRCL question 7.b) when release restrictions are therein identified. Indicate to which levels of information release restrictions apply. Make note in the chart if a level of information bears multiple restrictions (e.g. a portion of the SECRET information bears the caveat Canadian Eyes Only while the remainder of the SECRET information has no release restrictions.)

Canadian Information

Citizenship Restriction	PROTECTED			CLASSIFIED			
	A	B	C	CONFIDENTIAL	SECRET	TOP SECRET	TOP SECRET (SIGINT)
No Release Restrictions	X	X			X	X	
Not Releasable							
Restricted to:					X	X	
Permanent Residents Included*							

NATO Information

Citizenship Restriction	NATO UNCLASSIFIED	NATO RESTRICTED	NATO CONFIDENTIAL	NATO SECRET	COSMIC TOP SECRET
All NATO Countries					
Restricted to:					
Permanent Residents Included*					

Foreign Information

Citizenship Restriction	PROTECTED			CLASSIFIED			
	A	B	C	CONFIDENTIAL	SECRET	TOP SECRET	TOP SECRET (SIGINT)
No Release Restrictions							
Restricted to :							
Permanent Residents Included*							

COMSEC Information

Citizenship Restriction	PROTECTED			CLASSIFIED			
	A	B	C	CONFIDENTIAL	SECRET	TOP SECRET	TOP SECRET (SIGINT)
Not Releasable							
Restricted to:							

DND ONLY Embedded Contractor (Access to Controlled Goods)

Restriction	Yes	NO
SECRET clearance with CEO applies		

*When release restrictions are indicated, specify if permanent residents are allowed to be included.

Security Requirement Checklist (SRCL)
Supplemental Security Classification Guide

Part B - Multiple Levels of Personnel Screening: Security Classification Guide			
To be completed in addition to SRCL question 10.a) when multiple levels of personnel screening are therein identified. Indicate which personnel screening levels are required for which portions of the work/access involved in the contract.			
Level of Personnel Clearance (e.g. Reliability, Secret)	Position / Description/Task	Access to sites and/or information. Levels of Information to be accessed.	Citizenship Restriction (if any)
None	Project management Programmer analyst Electronics technologist Embedded system specialist – junior Embedded system specialist- intermediate Security of embedded system specialist Traditional information technology (IT) security specialist Software reverse engineer Wireless security specialist Laboratory technician Hardware security of embedded systems	No access to protected or classified information	
Reliability	Project management Programmer analyst Electronics technologist Embedded system specialist – junior Embedded system specialist- intermediate Security of embedded system specialist Traditional information technology (IT) security specialist Software reverse engineer Wireless security specialist Laboratory technician Hardware security of embedded systems	Access to the site and/or to sensitive information up to protected B	
Secret	Project management Programmer analyst Electronics technologist Embedded system specialist – junior Embedded system specialist- intermediate Security of embedded system specialist Traditional information technology (IT) security specialist Software reverse engineer Wireless security specialist Laboratory technician Hardware security of embedded systems	Access to the site and/or information up to the secret level	
Secret	Project management Programmer analyst Electronics technologist Embedded system specialist – junior	Access to the site and/or information up to the secret level	*Canadien*

Security Requirement Checklist (SRCL)
Supplemental Security Classification Guide

	Embedded system specialist- intermediate Security of embedded system specialist Traditional information technology (IT) security specialist Software reverse engineer Wireless security specialist Laboratory technician Hardware security of embedded systems		
Top secret	Project management Programmer analyst Electronics technologist Embedded system specialist – junior Embedded system specialist- intermediate Security of embedded system specialist Traditional information technology (IT) security specialist Software reverse engineer Wireless security specialist Laboratory technician Hardware security of embedded systems	Access to the site and/or information up to the top secret level	
Top secret	Project management Programmer analyst Electronics technologist Embedded system specialist – junior Embedded system specialist- intermediate Security of embedded system specialist Traditional information technology (IT) security specialist Software reverse engineer Wireless security specialist Laboratory technician Hardware security of embedded systems	Access to the site and/or information up to the top secret level	*Canadian*

Part C – Safeguards / Information Technology (IT) Media – 11d = non
IT security requirements must be specified in a separate technical document and submitted with the SRCL

OTHER SECURITY INTRUCTIONS

Insert instructions

Security Requirement Checklist (SRCL)
Supplemental Security Classification Guide