

The purpose of this amendment is to:

- A. answer questions posed by suppliers; and
- B. amend the numbering of the challenges in Annex B of the English CFP, there will be no updates to the French version.

All other terms and conditions remain unchanged

1. Can you confirm that a Lead Canadian Government Department is only required for Stream B (not required for Stream A).
  - a. Confirmed, A Lead Canadian Government Department is only required for Stream B.
2. Can you confirm that Stream A does not have partnership requirements?
  - a. Confirmed, Stream A does not have partnership requirements.
3. Regarding the resultant contract clauses. If we would like to negotiate a clause, when is the appropriate time to bring it up?
  - a. Resulting contract clauses can be negotiated after the project has been selected for funding.
4. Is completion and submission of the Part 5 – Certifications and Additional Information section required at the time of the proposal submission?
  - a. Canadian Content Certification must be received at proposal submission. The remainder of the certificates must be received prior to contract award.
5. We already have DG signatures for our project do we need to resubmit for signature?
  - a. A signature is a confirmation that the DG has read the document in full, and agrees to the collaboration of the organization as described in the project description and the budget information. Accordingly, a DG's signature must be dated no earlier than the date of the launch of the CFP, which is December 05th, 2016.
6. There is limited time available for the completion of this very complex proposal process due to Christmas and New Year's leave periods. Would Canada extend the proposal delivery date?
  - a. We appreciate the interest in the DRDC Innovation CFP. However, a draft of the CFP has been posted since October 6<sup>th</sup>, 2016 and no significant changes were made. The CFP will close on January 11, 2017. No extensions will be granted at this time.
7. How do I determine if my project is classified or not? Where can I get more information regarding this?
  - a. Proposals are to be deemed classified if they contain information related to the national interest that may qualify for an exemption or exclusion under the [Access to Information Act or Privacy Act](#) and the compromise of which would reasonably be expected to cause injury the national interest definition from the Supply Manual) in accordance with the Treasury Board of [Canada's Policy on Government Security](#). It is expected that the majority of proposals will not qualify for the exemption or exclusion and they will therefore be submitted as unclassified proposals.
8. Currently, we are working with an international company. Should all parts be made in Canada?
  - a. This procurement is conditionally limited to Canadian goods and Canadian services and there is no rating point attributed to the Canadian content. However, for each S&T Challenge, if there are two or more bids with a valid Canadian Content certification, the evaluation process will be limited to the bids with the certification; otherwise, all bids will be evaluated. Therefore, Bidders with a minimum of 50% of Canadian content must provide a valid Canadian Content certification with the proposal.

9. Can a new challenge be added to Stream B? The suggested wording is: S&T projects to re-establish a national base line for and revitalization of CBRN training for all first responders.
  - a. Several factors were considered for the determination of the S&T Challenges for the CFP including S&T priorities, budget, and comments received from stakeholders during the RFI period. There is no intent to add S&T challenges to Stream B.
  
10. Where is the letter template for partners?
  - a. There is no letter template and Bidders who wish to provide support letters from stakeholders can use their own template. However, Bidders submitting a proposal responding to stream B must include a completed Partner Signature Form as set out in Annex H. The Partner Signature Form template is downloadable from the online tool and can be found in the “list of annexes” section. Bidders should note that Support letters from named project partners will not be considered.

- B. amend the numbering of the challenges in Annex B of the English CFP, there will be no updates to the French version.

## Stream A

### Air Surveillance

- 1) Identify and assess innovative solutions and technologies for detection, identification, tracking and classification of airborne objects of interest like long range cruise missiles, long range aviation, and high speed manoeuvring weapons (<https://www.nap.edu/catalog/23667/a-threat-to-americas-global-vigilance-reach-and-power-high-speed-maneuvering-weapons>), including:
  - a) Identification and assessment of future sensing technologies and platforms (e.g. combinations thereof surface radar, air-borne and/or space-based electro-optical/infrared (EO/IR), over the horizon radar (OTHR), aerostat, forward deployed, reflective high power optics, passive radio frequency (RF), Electronic Intelligence, etc.) for detection and tracking of air targets;
  - b) Evaluation of radar technologies for long-range detection, tracking and cueing of air targets (with emphasis on the North), including technologies and signal processing techniques applicable to target detection such as bi-static Air Moving Target Indication (AMTI);
  - c) Consideration of environmental effects (e.g. RF clutter, cloud, aerosols, ionospheric and atmospheric properties and effects, etc.) on surveillance system performance;
  - d) Handling of multiple simultaneous airborne objects of interest;
  - e) Detection of long range cruise missile and high speed manoeuvring weapons launch; and
  - f) Pattern of life monitoring of foreign infrastructure.
- 2) Assess and mitigate surveillance system vulnerabilities (e.g. energy/power requirement, jamming, deception, capture, etc.).

### Surface Surveillance

- 3) Identify and assess innovative solutions and technologies for detection, discrimination, localization, classification and tracking of maritime surface objects using space, air, land, surface and subsurface platforms as well as relevant information resources. Of particular interest is:
  - a) Detection and improved discrimination of surface threats in presence of high vessel traffic, sea ice, debris, clutter, etc.;
  - b) Coverage, resolution and persistence of innovative solutions and technologies; and
  - c) Consideration of environmental effects on surveillance system performance.
- 4) Assess and mitigate surveillance concept vulnerabilities (e.g. energy/power requirement, jamming, deception, capture, etc.).

### Sub-Surface Surveillance

- 5) Identify and assess the viability and performance of existing and future surveillance solutions, technologies and methodologies for detection, localization, classification and tracking of underwater vehicles and other objects of interest to improve underwater warning and surveillance in blue water and littoral environments, including:
  - a) Long range deployable autonomous underwater/under-ice surveillance capabilities of increased endurance (months) and range (beyond 1000 km);
  - b) Surface and underwater/under-ice multi-function service “docking nodes” potentially housing charging stations (for deployable autonomous underwater/under-ice surveillance capabilities), communications, data processing, and sensors;
  - c) Consideration of environment on surveillance system performance;
  - d) Detection of underwater missile launch; and
  - e) Applications of airborne sensors to monitor underwater signals and communications.
  
- 6) Assess and mitigate surveillance concept vulnerabilities (e.g. energy/power requirement, jamming, deception, capture, etc.).

#### Sensor and Information Mixes

- 7) Projects involving the complementarity and interactions between disparate sensors and information sources in order to provide the flexibility for future acquisitions to determine the appropriate sensor and information mixes that deliver effective, responsive, resilient and affordable surveillance of Canada’s approaches including Canada’s Arctic region. This encompasses all identified environments (air, maritime surface and maritime sub-surface) including consideration of:
  - a) Identification and selection standard of sensor mixes and their placements on space, air, land, surface and subsurface platforms across all of the identified domains (air, maritime surface, maritime sub-surface);
  - b) Management and exchange of information of interest to DND/CAF across the identified domains to support strategic and operational decision making; and
  - c) Concepts of employment for layered surveillance systems and future joint strategic surveillance architectures.
  
- 8) Environmental effects on surveillance system performance including:
  - a) Assessment of the performance and limitations of the surveillance system in various environmental conditions;
  - b) Real time estimation of operational surveillance system performance in situ; and
  - c) Methods to limit environmental effects on surveillance system performance.

## Stream B

### Public Safety and Security

- 9) S&T projects that improve understanding of critical infrastructure (CI) vulnerabilities and their relative importance by better understanding and quantifying:
  - a) the risks associated with insider threats and mechanisms to mitigate this risk; or
  - b) the global impact and risk of counterfeit, fraudulent, suspect items (CFSI) to CI, including both hardware and software. Examples include nuclear power plants, aviation, transportation, medical equipment; or
  - c) the CI vulnerabilities associated with global navigation satellite system (GNSS) failures and how to mitigate those vulnerabilities; or
  - d) the risks and vulnerabilities with cyber-attacks related to connected vehicles, and how the cybersecurity posture of connected vehicles can be improved.
  
- 10) S&T projects that enable pre-event anticipation, prevention, detection, intelligence, and/or defeat of threats to CI by better understanding:
  - a) how to enhance intelligence and operations that strengthen Canada's ability to anticipate, prevent, and prepare for acts of cybercrime, terrorism and espionage by developing, testing, and validating new surveillance and interdiction technologies or analytical tools or systems that would assist national security, law enforcement and intelligence agencies and regulatory bodies in identifying criminals and criminal organizations terrorists, terrorist organizations, and individuals with malicious intent, their capabilities and the nature of their plans, and their supporters and counter the threat of proliferation of subject matter expertise; or
  - b) how the psycho-social aspects of risk perception among CI owners and operators (inclusive of cyber systems) can be improved to enhance CI resilience, for example through the implementation of specific risk mitigation measures.
  
- 11) Innovative S&T projects that enhance domain awareness in border regions, including air, land, maritime, remote and arctic environments, to support public safety and security partners and their priorities.
  
- 12) S&T projects that enhance the secure and efficient flow of goods and people at ports of entry by better understanding:
  - a) how to exploit data analytics techniques for automated targeting of cargo and travellers at the border; or
  - b) how to develop or evaluate screening technologies to detect weapons, explosives, contraband, currency or human trafficking; or
  - c) how to enhance the cyber security of international supply chains or traveller authentication systems; or
  - d) how to enhance the automation of traveller authentication and processing systems and cargo screening systems to reduce bottlenecks; or

- e) how to strengthen border security to prevent radiological-nuclear material smuggling and in particular enhance special nuclear material (SNM) detection.
- 13) S&T projects that investigate remaining gaps associated with locating, characterizing, and securing Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE) materials that are out of regulatory control.
- 14) S&T projects that generate field-deployable technologies to enhance non-intrusive stand-off detection and identification of non-traditional agents including toxic industrial chemicals (TICs) /toxic industrial materials (TIMs), homemade explosives and natural, synthetic or semi-synthetic opioids.
- 15) S&T projects which address threat from small unmanned aerial vehicles (aka “drone”), by experimental assessment of the effects of the drone impact on manned aircraft, or by development of capabilities or systems to protect against threats from small unmanned aerial vehicles (aka ‘drones’) against personnel, facilities, or critical infrastructure. The proposed developmental capabilities/systems must provide integrated detection, identification, and/or mitigation of the threat using any electronic or other means of detection, and using mitigation method(s) which pose no danger to bystanders.

Previous CSSP work has established performance and limitations of existing capabilities, as follows:

- Detection/Classification:
  - Radar – 1+ km detection, 500m classification by micro-doppler giving very low false alarm rate (FAR), 10+ second multi-sweep detection, azimuth and elevation indication, 10-20 deg vertical scan.
  - Electro-optical – 1 km detection with staring HD camera, fairly high FAR, requirement for high-contrast background, some capability for automatic classification but mostly requires operator confirmation.
  - Infrared – 300m detection with staring camera, see EO.
  - Acoustic – 200m detection, low detection rate and high FAR, easily masked by noise environment, rough azimuth indication.
  - Radio Frequency (RF) – 1+ km detection of proprietary protocols in 2.4 and 5.8 GHz bands, some identification of drone type, rough azimuth indication, not automatic. Not interested in 802.11 wifi protocol.
- Mitigation:
  - Counter-Drone Drone – net towed by other drone, net guns fired from other drone, manually flown onto target using first person view.
  - Launched Nets – 70m with parachute lowering, manually aimed and shoulder launched. Handheld net guns to about 25m with no parachute.
  - RF Spoofing – to about 1km, some ability to ‘crack’ proprietary protocol and provide control directions to the drone. Not automatic, not reliable.
  - Jamming – barrage jamming of RF and GPS signals to 700+ m, manually initiated, directional and 360 deg.

- System:
  - No integrated response chain, limited automated response, limited integration of different capabilities.
  - Poor user interface.

This Challenge will accept proposals which include at least one of the following:

- demonstrate significant improvement in the performance or reduction in limitations of capabilities listed above;
- demonstrate integration of capabilities into an automated response chain;
- identify and develop new capabilities not listed above; and/or
- provide capabilities with a significant reduction in cost.

16) S&T projects that examine data-driven and/or innovative solutions to reduce the accidental risks to first responders from being struck by vehicles while operating on roadways and in all-weather situations.

17) S&T projects that result in novel solutions that:

- a) apply wearable technologies to connect first responders and allow them to send and receive real-time actionable data during operations to identify and monitor threats, hazards and environmental conditions in which first responders operate; or
- b) protect non-specialist responders from hazardous or infectious substances with technologies that are built into their daily wear uniforms. The proposed technology could both alert first responders to contaminant danger as well as provide a minimum level of protection from the danger during the course of normal operations.

18) S&T projects that improve communications interoperability between first receivers (hospital emergency department personnel) and first responders during the triage of mass casualties, including the design of mobile applications that can be utilized to transfer critical information during an event.

19) S&T projects that support whole-of-society resilience to all-hazard risks through the development of specific methodologies and tools for community, regional, and national-level assessment of risk and resilience by:

- a. developing or enhancing risk-related datasets (e.g., exposure, vulnerability, disaster loss), models, and scenarios, as well as disaster resilience metrics on the local to the national scale; or
- b. developing risk assessments and geospatial systems that use datasets, models, or scenarios to represent or aggregate risks, are aligned with international best practice methodologies and standards (for example the United Nations Office for Disaster Risk Reduction (UNISDR) guidelines, databases and statistics), and enhance consistency across jurisdictions;

- 20) S&T projects that engage under-represented stakeholders such as youth, women, first nations, and persons with disabilities, using participatory action research methods, in order to leverage their strengths and to capture their special requirements in the development and evaluation of strategies for increased inter-disciplinary resilience that are scalable at the community, regional, and national level.
- 21) S&T projects that explore innovative approaches such as crowd-sourcing and social technologies for community engagement on specific local factors (e.g., economic, social, environmental and cultural); patterns; causes; or effects relevant to risk and resilience assessments.
- 22) S&T projects that strengthen the evidence base in support of disaster risk reduction (DRR), particularly for extreme weather events and climate change, and assist to establish a Canadian value on the return on investment (ROI) of DRR activities.
- 23) S&T projects that enhance the data collection and analytics as well as research that informs the prevention and mitigation of post-traumatic stress injuries (PTSI) in the first responder community.
- 24) S&T projects that innovate to improve preparedness against risks derived from extreme weather events and climate such as hazards monitoring and forecasting capabilities, early warning systems, emergency communication systems, that engage community-level stakeholders
- 25) S&T projects that help strengthen communities' resistance to extremist influences, and support effective evidence-based interventions and countermeasures to fight violent extremism and terrorism by:
  - a. investigating factors/dynamics related to families, peer networks, gender, trauma, and mental health; the investigation encompasses how they manifest both in terms of vulnerability/risk *and* mitigating/protective effects, with a view to develop screening/assessments to inform programs to prevent, intervene or disengage and re-integrate vulnerable individuals; or
  - b. exploring how broad social, economic, political, and demographic trends manifest at local levels and affect communities, either negatively through increased threat of radicalization to violence or other types of serious crime, or positively through 'resilient' forms of reaction, such as community based efforts towards integration, support to vulnerable community members, reconciliation, and peace-building; or
  - c. leveraging lessons learned from public health research and practice about effective interventions to influence behavior at the population, community and individual level (interventions that range, for example, from broad public awareness campaigns to best practices for managing cases involving mental health and addictions), in order to support efforts in countering radicalization to violence and preventing involvement in other forms of serious crime.