Applicant Guide for the
Counter Uncrewed Aerial Systems (CUAS)
Sandbox 2026

September 14 to October 9, 2026
Suffield Alberta

Seeking CUAS solutions that can detect and/or defeat Micro and Mini Uncrewed Aerial Systems (UAS) with systems that can be integrated into the broader military command and control systems.

Threat drones are evolving, and we need continual advancement in solutions to counter them.

Major changes from CUAS 2024:

- More test time each day (page 7)
- Nighttime testing available (page 7)
- "On-Deck" pre-testing setup available (page 8)
- Post-selection technology substitutions modified (page 13)
- Command and Control communication protocols (Annex A, page A-2)
- New operational scenario: Monitoring and defending a linear border (Annex A, page A-4)
- Tethered drones – A new threat requiring new solutions (Annex A, pages A-5, A-8, A-11)
- Royal Canadian Mounted Police areas of interest added (Annex, page A-11)
- Risk evaluation modified (Annex B)
- Diamond in the Rough prize process updated (Annex C)

Due to the importance of CUAS, the Department of National Defence (DND) and Canadian Armed Forces (CAF) have multiple CUAS activities underway. Companies who have applied to or been accepted under a different CUAS activity are eligible to apply to CUAS 2026. The selection process will consider the implications between different activities. See page 2 for details.

IDEaS IDEeS
INNOVATION FOR DEFENCE EXCELLENCE AND SECURITY
INNOVATION POUR LA DÉFENSE, L'EXCELLENCE ET LA SÉCURITÉ

Table of Contents

Please note that in the event of any discrepancy between the information in the downloadable documents and the IDEaS website, the downloadable documents take precedence unless otherwise indicated.

CUAS Sandbox 2026 eligibility and how to apply

Eligibility for an IDEaS Sandbox - Who can apply?

Applications are open to individuals, academia, not for profit organizations, and industry of any size, as well as provincial, territorial, and municipal organizations.

Federal government departments/agencies, and federal Crown Corporations are not eligible to submit applications to this Call for Applications (CFA).

Foreign companies can apply – in previous Sandboxes as much as 50% of the selected companies were from outside Canada. Sandboxes are not exclusively restricted to made in Canada products/solutions; however, the level of Canadian content within each application will be given consideration during the strategic selection process.

Eligibility and ownership of the solution's intellectual property (IP)

The applicant must own the IP of the solution. In this context, it is recognized that a solution may contain multiple sub-components, and the applicant may not own the IP of all sub-components. In such cases the innovation and the IP of concern to IDEaS is for way the components are integrated with each other, creating the IP for the solution in total.

This does not prevent the applicant from partnering with others, or using marketing or sales companies to assist in their application, act as their point of contact, and attend the sandbox as part of a technical team, but the applicant applying to the sandbox and attesting to the application must be the owner of the solution's IP, must comply with all requirements related to the sandbox even if executed by their partners, and will be the recipient of any consequential funding from IDEaS. Distribution of any such funding to any partners is at their discretion unless otherwise specified by IDEaS.

Eligibility and the Canadian "Policy on Sensitive Technology Research and Affiliations of Concern"

On February 14, 2023, the federal government announced its intent to further protect Canada's research, its institutions, and its intellectual property by announcing that Canada would adopt an enhanced posture regarding Canada's research security.

While the policy focuses on grants and funding with universities and research institutions, the IDEaS program utilizes the policy and its tools of Sensitive Technology Research Areas and Named Research Organizations to ensure that companies selected to participate in the sandbox meet the spirit of that policy with its two-step validation process summarized below. Companies that do not meet this requirement may not be eligible to attend the sandbox.

Note that in the sandbox application form, "*Section 9: Terms and Conditions of Applying to and Participating in the Sandbox*", applicants are asked to make a proactive statement about all affiliations with any of the Named Research Organizations.

In a practical sense, aside from answering the question in Section 9 of the application form, implementing this security validation is only done on the companies after they are provisionally selected to attend the sandbox, and as will be detailed in their acceptance letter.

Step 1: Determine if the selected solution's technology advances any sensitive technology research area.

- If the proposed solution will not aim to advance any of the listed Sensitive Technology Research Areas, no further steps are required under this policy. Solutions that will merely use an existing technology are not included in this policy.

- If the proposed solution will aim to advance any of the listed sensitive technology research areas, companies must attest that they are not affiliated with, or in receipt of funding or in-kind support, from any of the institutions on the list of Named Research Organizations.

Step 2: Check sandbox participants affiliations
All companies selected to attend the sandbox must review the list of Named Research Organizations. If a company is affiliated with, or in receipt of funding or in-kind support, from one or more of the institutions on the list of Named Research Organizations, they may be required to terminate those connections in order to continue as a participant in the sandbox.

Can technologies that applied to or were accepted into other DND/CAF CUAS projects apply to CUAS 2026?

The importance of CUAS is resulting in multiple overlapping DND/CAF sponsored CUAS activities that may or may not be under the IDEaS program.

Companies who have applied to or been accepted under a different DND/CAF CUAS activity are eligible to apply to the CUAS 2026 sandbox with those or other technologies, noting that:

- Section 9 of the Sandbox Application form requires all companies to declare all prior or ongoing demonstrations of their technology or variants of it to DND/CAF. This includes the space to describe what change(s) have been made to a technology since all prior demonstrations, making a case for why DND/CAF should select it to see it again at the sandbox.
- No selection advantage is given based solely on the fact a company was or was not selected for another CUAS activity.
- Other CUAS activities may already include opportunities for demonstrations to DND/CAF without the sandbox. On a case-by-case basis that factor, and any results, will be considered in our selection decisions for CUAS 2026.

Technology Readiness Level (TRL)

IDEaS need to ensure that solutions are ready for the near-end state demonstrations and testing in a simulated environment that DND/CAF expects in a Sandbox. Learn more about Technology Readiness Levels (TRLs).

At a minimum, at the time of application your solution must have

- already successfully completed the work and validation testing associated with TRL 5, "*Validation - refined integration of applications and/or concepts to confirm validity.*"

or

- already successfully completed the work and validation testing associated with TRL 4, "*Proof of concept - basic integration of applications and/or concepts to demonstrate viability*"; and
- include is a reasonable plan with your application to complete TRL 5 prior to May 15, 2026.
- Failure to achieve TRL 5 by that date may constitute grounds for any sandbox offer to be rescinded. The letter of provisional acceptance into the sandbox will detail the ways and means to demonstrate compliance with this TRL 5 requirement.

How to Apply

Step 1: Read this Applicant Guide for all the information on the challenge, Sandbox, criteria, selection, test plans, your responsibilities, funding, and other information.

Step 2: Download and complete the following:

Important note: Several of these forms are fillable PDFs that WILL NOT FUNCTION if you open them from a web-based version of Adobe. If you get any sort of error or cannot open the forms:

1. **Download the forms to your local computer.**
2. **Open them with a desktop version of Adobe. Your default may be set to open it via your web browser which may not work. If so, in Windows Explorer right click on the file name, select "Open with", and then select Adobe.**
3. **After they open, look for a yellow bar at the top. Depending on your settings, you may need to enable JavaScript: If seen in the top yellow bar, click on "Options" and then "Enable".**

- **The Application Form**. This is a multiple-choice short answer series of questions used to describe your solution. The questions are the technical criteria used for evaluating your application to attend the Sandbox. The instructions, scoring metrics and weight factors are included within the form.

- **The Test Plan Template**. This tells us what you are proposing to show us during your time in the Sandbox, enabling us to ensure that your plan aligns with the intent of the Sandbox and that the Sandbox is suitably equipped and ready for your arrival.

- **Radio Frequency Spectrum, DND 552**. Only if your solution emits any RF energy you must submit an "Application for Spectrum Supportability" DND Form 552, as part of your application. DND/CAF will use this to determine if the RF usage is supportable in the Sandbox. See Section 6 of the application form for additional details and technical assistance on this topic, as well as the DND 552 form itself.

- **Company and Technology Overview "one-pager"**. This is a PowerPoint one-pager provide DND/CAF with a brief description and photographs of the company and their technology in order to create a compendium of the applying companies and solutions. It will also be used to create briefing packages for visitors to the Sandbox and other communications purposes.

Step 3: Request a “PriviDox” account, the submission portal for your application.

PriviDox is a secure file transfer service used to submit your application documents to IDEaS. There are no fees to you for using this service.

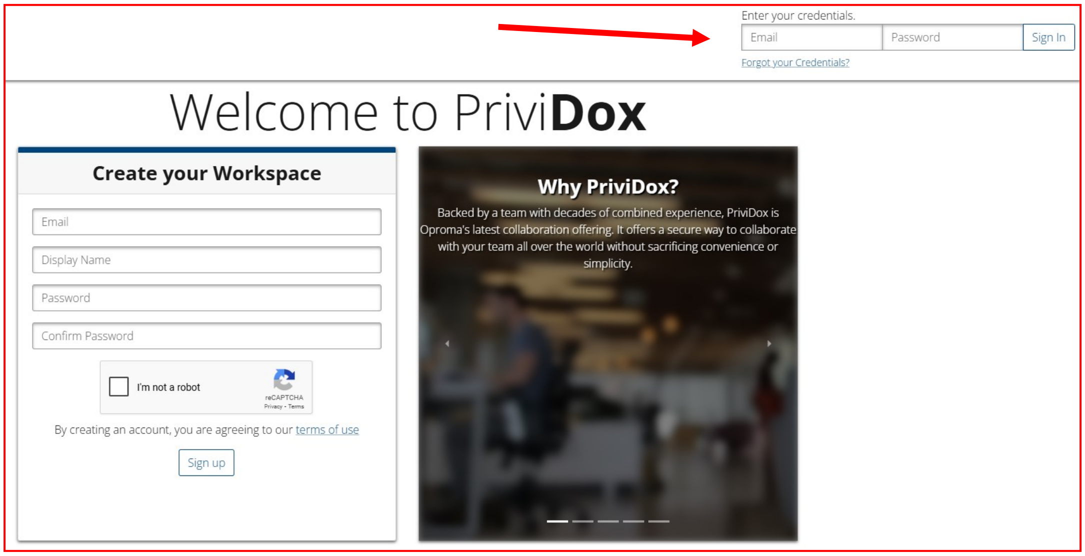
PriviDox is based on user accounts identified by a valid email address, with a password that you create when you activate your account. Only that account can see your company’s documents you submit to us. Other companies cannot see your documents.

PriviDox accounts will only be made available after October 1, 2025.

To request a Prividox account with IDEaS for this Sandbox:

- Email us at DEaSSandboxes-environnementsprotegesIDEeS@forces.gc.ca requesting a PriviDox account.
- Include the email address you want your account to be called. All correspondence exchanging files will go through that account.
  1. Within two business days you will receive two automated emails from PriviDox inviting you to “*Activate*” your account, and to “*Start Collaborating*” with the CUAS 2026 Sandbox.
  2. Wait to receive those emails before trying to access your account. Check your account and spam for emails from PriviDox <no-reply@prividox.com>. Follow the instructions in those emails.
  3. Make sure you use your email address when you login to PriviDox as it is linked to the PriviDox space we have made for your company.

- When logging in to Prividox enter your account in the top right corner of the login page.
  (**DO NOT use the centre “Create Your Workspace” area**.)



By creating an account, you are agreeing to our terms of use

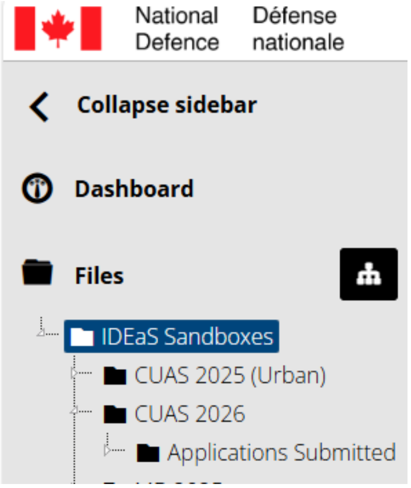
Backed by a team with decades of combined experience, PriviDox is Oproma's latest collaboration offering. It offers a secure way to collaborate with your team all over the world without sacrificing convenience or simplicity.

Step 4: Submit your application prior to the closing date as posted on Counter Uncrewed Aerial Systems Sandbox 2026 - Canada.ca using your PriviDox account:

- Once your account is activated (see Step 3 above):

1. Login to your PriviDox account **in the top right corner of the login page**. (**DO NOT use the centre "Create Your Workspace" area**.)

2. Once logged in, look on the left side menu bar and click on "Files".
   - Then click in the subfolders until you are in the "Applications Submitted" folder.
   - You should only be able to see an "Applications Submitted" sub-folder for your company.
   - Click on your company's sub-folder.



3. **In your company's named sub-folder, drag and drop all of all your application files:**
   - Company and technology overview "one-pager";
   - Application Form;
   - Test Plan Template;
   - Radio Frequency Spectrum Form, DND 552 (if applicable); and,
   - An untouched three minute or less real video.

4. You can delete and change the files you've uploaded up until the closing date posted on Counter Uncrewed Aerial Systems Sandbox 2026 - Canada.ca.

5. Send us an email when your submission is completed.

6. We will send you an email verifying we have received your documents.

- For any technical issues with Prividox, please contact support@prividox.com.
- For queries about the Sandbox, or if you haven't received your PriviDox account within two business days, please contact IDEaSSandboxes-EnvironnementsprotegesIDEeS@forces.gc.ca.
- Note that your access to the account may be closed after the application period is closed.

We look forward to receiving your CUAS 2026 Sandbox application!

When will I be told if I am selected to attend the Sandbox?

You will be notified by email of your evaluation results and selection status approximately six to eight weeks after the CFA closes. The selected applicants will have five business days to accept their invitation. This will give several months or pre-Sandbox notification and preparation.

Should a selected applicant not accept their invitation, or withdraws their acceptance, or is removed from the Sandbox process, additional offers to other applicants may be made under the same selection process at DND/CAF's discretion and providing sufficient time is available before the Sandbox commences.

CUAS Sandbox description

Overview

Successful applicants will be invited to demonstrate their solutions to this CUAS challenge at CFB Suffield, Alberta, September 14 to October 9, 2026, noting that the selected participants are only present for their specific two to five days within that window. The DND/CAF will provide a well-equipped and fully staffed test environment specifically designed for that challenge with such things as test articles, weapon ranges, airborne targets, imagery, data collection, and operational scenarios, as well as work and storage space, security, etc. We also provide on-site military, Royal Canadian Mounted Police (RCMP), US Department of Defence (IWTSD) and DND/CAF science experts, as well as other government safety and security potential users, to give innovators observational feedback on their solutions.

There are no fees to the innovator for using the Sandbox.

Innovators operate their own prototypes for their desired test and demonstration plan, receiving on-site immediate feedback from our end-users. It is not a Contest with multiple innovators publicly competing with each other and an isolated panel of judges. Instead, we are seeking proactive continuous one-on-one engagement.

Collectively, this CUAS Sandbox provides a venue for:

- Innovators to refine and develop their prototype during and after the Sandbox, including iterative testing and on-site improvement while concurrently receiving direct feedback from DND/CAF/RCMP/IWTSD.
- DND/CAF personnel to learn about the state of possible future upcoming solutions to the challenge, potentially influencing future DND/CAF acquisition decisions.
- Selected allied military and security partners to DND/CAF may also be present, expanding the exposure an innovator may receive during and after the Sandbox.
- Interaction and discussion with others in the field of work.

How does the Sandbox process work in general?

- The CFA is usually published six-nine months in advance of the Sandbox.
- An evaluation and selection process determines which innovators are accepted.
- After selection, DND/CAF and the selected innovators complete their pre-Sandbox preparations, shipping, and travel to attend the Sandbox.
- The Sandbox is conducted.
- Post-Sandbox reporting and administration with each innovator is completed.

What’s provided in the Sandbox?

DND/CAF will provide the following at no cost to the participants:

- A test area of suitable boundaries and airspace control for the planned activities including the operation of drones, limited electronic signals, and weapons. Precise details and sizes will depend on the proposed solutions that are selected for the Sandbox, commensurate with safety, environmental, and other considerations.

- Various UAS targets operated by our Red Team, representative of those encountered in the operational scenarios.
- A limited variety of small portable antennae mounting masts are available, approximately 1.5 – 3 metres (5-10 feet high). These could be used for temporarily mounting small sensors for example. The participant would be responsible for any required mounting hardware and tools.
- For solutions choosing to demonstrate mobile capability a gravel road will be available, however the participant will be responsible for providing an appropriate vehicle on which their system is safely mounted for such mobile demonstrations.
- Escorts for site transportation.
- Communications equipment.
- Some pre-existing inventories such as tables, chairs, fridge etc.
- Materiel Handling Equipment (MHE) such as forklifts or small cranes if required.
- Lockup facilities for each participant's equipment, with on-site security.
- Office facilities including phones, computers and WIFI.
- Data collection equipment if feasible and subject to the type of solution.
- Limited photography/video services.
- DND/CAF will provide observers for each test. Participants will receive all test data, photographic and video imagery, as well as any pertinent feedback, for their solution, subject to any security classifications and approvals that may arise.
- Lunches and coffee breaks.
- If requested in Section 6 of the Application Form, additional resources may be made available at DND/CAF's sole discretion on a case-by-case basis.

What happens during the Sandbox itself?

Selected innovators are given two to five days of testing time at the Sandbox. Applicants can indicate their preferred dates to attend in the Application Form; however, the precise dates given to each participant are at DND/CAF's sole discretion and are non-negotiable.

Innovator demonstrations are isolated from each other to protect intellectual property and prototype performance.

Our military, RCMP, IWTSD and DND/CAF science experts are paired with each innovator for interaction during your testing, including daily debriefs and a final debrief upon completion of your testing.

The Sandbox Red Team will fly representative UAS threats and operating scenarios to be demonstrated against, adjusting based on the capability of each CUAS system.

The Test Plan template contains a more detailed description of the likely scenarios that will be available. Final test plans will be designed through consultation with the selected participants to exhibit the capabilities and explore the limitations related to each technology. Actual target UAS will be subject to change based on availability.

Data collected from the target UAS and participant countermeasures will allow the calculation of range, accuracy, and time, to be used as performance outputs and reports for both the DND/CAF, as well as the participant. Participants only see demonstrations, results, and reports of their own technology.

What's the Sandbox schedule for a specific participant?

A detailed schedule will be developed with each selected participant prior to the Sandbox, based on the following expectations:

- Arrive at your hotel prior to Day 1.
- Depart for the test range at 0700 each day (one hour transit each way).
- Workdays will be 8 am to 6 pm (to be confirmed).
  - For CUAS 2024, workdays concluded at 4 pm but many participants asked for more testing time, especially as setup and calibration can consume a significant part of each day. For CUAS 2026, the workday is provisionally extended to 6 pm each day. This will be discussed during final planning to confirm the benefits and viability of doing this.
- Day 1 will entail suitable in-briefs, unpacking, and calibration.
- Demonstrations may commence on Day 1 if time permits.
- Lunch/breaks will be provided on-site to maximize testing time.
- Securing of all equipment will be completed prior to departure each day.
- Days 2, 3, 4, and 5 (if used) conducted as per the DND/CAF approved Test Plan.
- Final Day:
  - All tests will be concluded by 12 pm.
  - A verbal out-brief by the Sandbox SMEs will be conducted with the participant. Provision of test data and written information will follow later.
  - A full pack up and departure of the participant's materiel and personnel must be completed by 4 pm of that day.
- Departure date/time after the Sandbox is at the participant's discretion.

Can nighttime testing be done?

A limited number of previous Sandbox participants have asked if nighttime testing could be included. CUAS 2026 will be primarily conducted during daylight hours and that is the expectation with each company selected; however, once a company is selected, we are open to considering portions of their Sandbox time at night within the following post-selection process and considerations:

- Companies are to indicate a desire for night testing on their test plan submitted at the time of application.
- There must be a substantive testing benefit and technology difference between testing in day versus night conditions such that the extra effort and resources for nighttime testing is of sufficient value and worthwhile.
- If the results of daytime testing can be sufficiently inferred to how a system would perform at night, nighttime testing will generally not be supported.
- Notionally, but subject to negotiation, when night testing is conducted:
  - There would likely be no daytime testing that day as the Sandbox staff for that test lane will work a night shift instead.
  - The work period would be approximately 1600 hours to 2359 hours (sunset is at 1800).
- Details of the above would be negotiated after initial selection and pre-Sandbox. Canada will make all reasonable efforts to accommodate the request where possible. Note that this may include the advantages, disadvantages, and interdependencies of having multiple test sites concurrently done at night or not.
- Canada retains the authority to determine final approval to proceed or not with nighttime testing at its sole discretion.

Pre-test date “On-Deck” unpack and setup?

The transportation, unpack, and setup of technologies at the Sandbox varies greatly. As the actual test time on the range is of high value, some previous companies have asked for additional unpack and setup dates before their starting date on the range. This is usually not possible as the test range is still occupied by the previous company who need to pack and leave before the next company can unpack which is the normal sequence of events we expect.

However, after a company is selected to attend the Sandbox, Canada is open to discussing reasonable requests for additional time and space to unpack technologies prior to the Sandbox test day #1:

- If doing so will save a significant amount of setup time on Day 1.
- It can be done on a non-interference basis with other companies.
- If the unpack is done at a location other than the actual test site, final movement to the actual test site is viable without compromising the pre-setup advantages achieved.
- The unpack and any validation/calibration can be accommodated in a safe and acceptable manner at the pre-test location.
- Requests will generally be limited to systems that were disassembled for shipping and need to be reassembled and are easily moved to the actual test range (for example, vehicle mounted weapons).
- Systems that are smaller or have mechanically independent components that are connected by cables once on the test range (such as multiple sensors on tripods that will have to be re-packed again anyway) are less likely to be accommodated.

Canada will make a reasonable effort to accommodate all such requests; however, it is on a case-by case basis and Canada retains the sole discretion to agree or not to any pre-test date unpack and setup.

CUAS 2026 “Diamond in the Rough” Prizes (see Annex C for details)

The Diamond in the Rough prizes are awarded for CUAS innovations tracking towards success with good growth potential and impact to receive financial non-repayable grants. With consideration to the potential and impact, prizes will be awarded for up to the following notional amounts. Final prize amounts will be established to align with the developmental potential of the selected technologies.

1st Place	up to $1,000,000
2nd Place	up to $500,000
3rd Place	up to $250,000

Please refer to Annex C for the detailed description, criteria, and selection processes.

What happens after a Sandbox?

After the Sandbox is concluded a written report will be provided to each participant documenting the observations from DND/CAF on only the participant’s solution.

DND/CAF will internally consider the observations they made at the Sandbox to monitor any progression towards solving the specific challenge and how that may or may not influence further force development planning, procurement, priorities, and other considerations internal to IDEaS and across DND/CAF.

Attendance at a Sandbox, or even successful demonstrations within the Sandbox, does not imply any intent or commitment that DND/CAF will undertake any further activity with any solution or organization. It is completely up to the participant what they do with the information learned during the Sandbox.

Will there be another CUAS Sandbox after 2026?

Yes. IDEaS is planning to conduct a CUAS Sandbox every two years for the near-term future, noting that after each is concluded the decision to conduct the next will be confirmed.

Criteria

Sandbox criteria vs end-state operational requirements: The criteria used for this Sandbox represent the limitations and desired characteristics in order to prioritize and select the accepted participants to the Sandbox only. They do not represent final operational requirements for any current or future DND/CAF procurement program which may be quite different.

What are the criteria and how are they scored?

- The multiple choice/short answer questions on the Application Form are used for describing your solution and evaluating your application to attend the Sandbox. Many of the questions are for descriptive purposes only and are not criteria and are not scored. Those that are scored and used as criteria are clearly marked as such, including its specific scoring metrics.
- The evaluation method and total score calculations are explained on Page 4 of the form.
- The list of the technical criteria and their relative weighting factors is on Page 5 of the form.
- A solution that does not achieve a PASS on all mandatory criteria in Section 1 of the form will not proceed further in the evaluation process and will not be selected to attend the sandbox.

Solution categories

On the Application Form, solutions are described under one of the following three categories, and selections to attend the Sandbox may be made from each category:

- **Detect Only.** These are solutions that have the capability to provide the detection that a UAS threat has appeared, but do not include a capability to defeat the UAS in any way.
- **Defeat Only.** These are solutions that do not have the capability to do the initial detection that a UAS threat has appeared, but once cued to that threat by a separate Detect system do have the capability to target and defeat those detected threats.
- **Detect and Defeat.** These are solutions that can both detect the appearance of a UAS threat and defeat it.

This does mean that solutions in the different categories are responding to different sets of criteria which may result in different potential maximum numerical scores. However, selections of who comes to the Sandbox are made separately within each category. Therefore, applicants are competing against those in the same category with the same available scores.

Selection

Acceptance into the pool of qualified applications

Following the evaluation of all technical criteria, all applications that that meet the eligibility requirements described earlier and achieve a “Pass” on all mandatory criteria and all minimum mandatory scores (if any) are placed into the pool of qualified applications. There is no minimum overall score required.

Read the Criteria section for a full description of all criteria and how they are scored. Acceptance into the pool of qualified applications does not constitute an invitation to participate in the Sandbox. Applications that do not qualify for the pool will not receive any further consideration for attending the Sandbox.

Science and technology risk assessment

- In seeking innovative solutions, the IDEaS program is open to high-risk untested solutions, provided such solutions come with reasonable substantiation and a high impact to addressing the challenge at hand. High risk without high reward is of less interest.
- For CUAS 2026, once a technology is identified for potential selection the evaluation/selection team will consider the need for a full and formal science and technology risk assessment of the solution.
    - If the selection decision is not in doubt regardless of the risk, no further risk assessment is required and the selection can continue.
    - If the selection decision is in doubt due to the risk, a full risk assessment may be conducted as described at Annex B and the outcome will be incorporated into the final selection decisions.

Selection of the Sandbox participants from the pool of qualified applications

- All qualified applications in the pool will proceed to be considered against the standardized IDEaS Strategic Selection Parameters (SSP) as described here.
- Applicants do not provide any additional information to respond to these parameters. They only provide the information as described in the Application Form.
- Selection of the applications is at the sole direction of the Challenge Steering Committee. Applications that achieve a full technical score are not guaranteed selection for participating in the Sandbox.
- The committee will consider the evaluation results of the applications and examine the distribution of selections against the following parameters, listed below in no particular order:
    - Alignment with priorities – Aligns with current and emerging departmental and/or Government of Canada priorities.
    - Alignment with DND/CAF – Aligns and integrates within the DND/CAF, i.e., the solution integrates with departmental military systems, doctrines, standard operating practices.

- Operational investment – Considered worthwhile for investing operational resources (e.g., personnel, equipment, data, budget, etc.) to implement the solution.
- Distinction of solution – Does not duplicate previous/existing/planned work of Canada and its Allies known at the time of evaluation.
- Strength and risk of Application – The strength of an individual application and the related risk, represented by:
  - The solution's point rated scores as described in the Application form, including the cumulative score and scoring on individual criteria; and
  - The risk assessment as described above, including Annex B if applicable.
- Impact – The application's potential to be a disruptor in the field of the Challenge and/or S&T domain.
- Type of solution – Allows DND/CAF to select a balance across solution categories, methodologies, and various applicable military environments. For this Sandbox, and subject to the number and type of qualified applications received, selections may be dispersed across the following categories:
  - **Detect Only**. These are solutions that have the capability to provide the detection that a UAS threat has appeared, but do not include a capability to defeat the UAS in any way.
  - **Defeat Only**. These are solutions that do not have the capability to do the initial detection that a UAS threat has appeared, but once cued to that threat by a separate Detect system do have the capability to target and defeat those detected threats.
  - **Detect and Defeat.** These are solutions that can both detect the appearance of a UAS threat and defeat it (as described above) in a seamless comprehensive system.
- Industrial and Socio-Economic benefits to Canada.

Companies with multiple applications

The guiding intent is that a company gets a single demonstration period at the Sandbox, even if they submit multiple applications for different technologies. To achieve this effect all applications a single company submits will initially be evaluated and considered for selection independently; however, once any one of those applications is selected:

- All other applications from that company will be disregarded until such time as all other applications from all other companies have been considered;
- Unless an exemption is made based on the Strategic Selection Parameters, the demonstration period for the company will not exceed the already established five days maximum for any single participant, and only with time permitting and subject to DND/CAF's approval, demonstrations of the company's other technologies may be permitted.

Multiple submissions from one applicant are permitted, provided the solutions are thoroughly different from each other and not simply a variation of the same method or technology. Each solution must be submitted with its own complete application package. The determination of the degree of difference and acceptability of each additional submission shall be at the sole discretion of DND/CAF.

After a company is selected and invited to attend the Sandbox for a specific technology, it will be allocated several Sandbox days to conduct its demonstration. If the company submitted multiple applications, it may be permitted, to bring its other technologies for additional demonstrations but without any increase in total Sandbox days. Permitting such additional demonstrations shall be at the sole discretion of Canada.

Invitation and acceptance

The selected applicants will receive a formal letter of invitation via email to participate in the Sandbox and will then have five business days to accept the invitation and any supplemental terms and conditions it may include. Note that:

- The basic terms and conditions for attending each Sandbox are specified in Section 9 of the Application Form.
- Additional supplemental terms and conditions may be imposed as a result of the evaluation of an individual application. For example, there may be a special safety protocol imposed due to the nature of an applicant's solution and the desired testing/demonstration.

Should a selected applicant not accept their invitation, or withdraws their acceptance, or is removed from the Sandbox, additional offers to other applicants may be made under the same selection process at DND/CAF's discretion and providing sufficient time is available before the Sandbox commences.

Technology demonstrated and any substitutions

Once a company has accepted their invitation the company is expected to focus on and first demonstrate the technology they were selected for, even if additional demonstrations of other technologies are included. If the selected technology in whole or part is no longer being demonstrated at the sandbox, the company must advise Canada of such changes in advance of the sandbox, the reasons, and any proposed substitutions or mitigations. At Canada's sole discretion, the offer to participate in the sandbox may be rescinded. This is to ensure that there continues to be a demonstration of sufficient value to Canada.

Test Plans

Effective and efficient use of the Sandbox is enabled when the proposed demonstrations and testing are:

- Collaboratively optimized between DND/CAF and the participant attending the Sandbox.
- Safely possible within the Sandbox's environment and provided resources.
- Relevant to the challenge; and
- Of interest to DND/CAF.

To enable that determination each applicant must submit their completed Test Plan Template as part of their application:

1. The Test Plan Template includes detailed instructions on any constraints and restraints for developing a proposed plan.
2. The Test Plan will be evaluated as a Pass/Fail criteria, as per Section 6 of the Application Form.
3. DND/CAF will be the sole authority for final approval of the participant's test plans:

  - If portions of a proposed test plan are not acceptable to DND/CAF, the offer of acceptance to attend the Sandbox may impose changes to the test plan that the participant must accept if they agree to attend the Sandbox.
  - After a participant is selected, additional refinement and detailed scheduling of the proposed test plan may occur to optimize use of the Sandbox for each participant. Such changes will remain within the overall intent of the original plan.
  - Final approval of all test plans will be at the sole discretion of DND/CAF.

Responsibilities

- Read and accept all Terms and Conditions in Section 9 of the Application Form.
- It is emphasized that participants agree to abide by all reasonable safety and security protocols that may be imposed during the Sandbox, including those related to COVID-19. Participants are responsible to ensure they and their equipment meet and follow all entry or transit requirements imposed by all applicable authorities for their itinerary to arrive at the Sandbox location ready to commence their demonstrations on schedule.
- Participants are responsible for arranging all transportation, shipping, food (except lunch at the Sandbox site), and lodging of all their equipment and personnel to, from, and during the Sandbox.
- Participants are responsible for all maintenance, tools, parts, and technical support required for their solution during the Sandbox.
- Participants are to complete all tasks as per Section 9 of the Application Form.
  - Tasks to be completed prior to the Sandbox (administration and planning).
  - Tasks to be completed at the Sandbox (safety and demonstrations).
  - Tasks to be completed after the Sandbox (administration).
- Refinement of these generic tasks will occur with each participant after acceptance to attend the Sandbox is confirmed.
- Failure by the participant to complete any task on schedule constitutes grounds for removing the participant from attendance at the Sandbox.

DND/CAF will be responsible for all pre-Sandbox coordination with the participants, the provision and functioning of the Sandbox, and the post-Sandbox administration. Note that much of this is conducted by the DND/CAF contractor for organizing the Sandbox events. Participants can expect to be contacted by the contractor after accepting an invitation.

Funds

Funding provided for travel, accommodations, living, shipping, and consumables

DND/CAF is providing the test environment at no cost to participants; however, DND/CAF recognizes there are costs incurred by participants to attend the Sandbox. Funding is provided via one of two administrative methods:

- For companies incorporated in Canada, a government grant of $20,000 CDN will be given, regardless of actual costs.
- For companies not incorporated in Canada:

- IDEaS is not authorized to issue grants to such companies. Instead, such companies will receive a contract up to a maximum of $20,000 CDN supported by receipts for only the following types of expenses:
    - Travel, accommodation, and living expenses. The National Joint Council Travel Directive will apply for any travel, accommodation and living expenses. https://www.njc-cnm.gc.ca/directive/d10/en
    - Shipping and transportation expenses of equipment to/from the Sandbox location and the company's location.
- If such costs are less than $20,000 CDN, the lesser amount will be paid.
- All other costs (such as but not limited to parts, maintenance, wages, etc.) are not reimbursable.

Miscellaneous

Helpful definitions

Innovators: The innovation community at large.

Applicants: Those innovators that complete and submit an application to a specific Sandbox when it is offered.

Applications: The information form(s) submitted by an applicant for a specific Sandbox.

Participants: Applicants who have been selected, received, and accepted a confirmed invitation to attend an actual Sandbox. Note that a participant is the organization and may send multiple personnel to a Sandbox.

Test Environment: The physical or virtual environment in which demonstrations are conducted.

Technology Readiness Levels (TRLs)

- TRL 1: Identification—basic principles and/or properties are observed.
- TRL 2: Definition—practical applications and/or concepts are formulated.
- TRL 3: Observation and Analysis—analytical and/or laboratory research and/or experiments are undertaken.
- TRL 4: Proof of Concept—basic integration of applications and/or concepts to demonstrate viability.
- TRL 5: Validation—refined integration of applications and/or concepts to confirm validity.
- TRL 6: Simulated Demonstration—near-end state solution is demonstrated and tested in a simulated environment.
- TRL 7: Real-World Demonstration—near-end state solution is demonstrated and tested in an appropriate real-world environment.
- TRL 8: Qualified Solution—end state solution is completed and refined through testing.
- TRL 9: Proven Solution—final solution is implemented and proven successful.

Intellectual property

The participant retains full ownership and control of the solution being demonstrated and its intellectual property. See additional detail on the IDEaS FAQ page.

Security requirements

A formal security clearance to participate in the Sandbox may be required. Participants will always be under appropriate escort while on DND/CAF property.

Access to the Sandbox test site may impose certain physical, communication, and electronic restrictions on participants which will be detailed prior to the participants arrival at the Sandbox.

Participants will need to provide lists and descriptions of all personnel and equipment being brought to the Sandbox for security screening purposes. The following information will be required once a participant is selected:

- Copies of passports and birth certificates; and
- Visit Clearance Requests.

Participants will need to permit security verifications and background information on their personnel that attend the Sandbox. If the security process reveals that a particular person(s) will not be permitted to attend the Sandbox, discussions, alternatives, and mitigations will be discussed with the participant to try and resolve the issue(s). If the issues cannot be resolved, the invitation to attend the Sandbox may be withdrawn.

Security screening criteria will depend on, in part by innovator residence and proposed Sandbox venue.

For any participants whose proposed solution includes controlled goods (see section below), additional security aspects may be imposed, if necessary, on a case-by-case basis.

Controlled goods

The participant must identify any Controlled Goods used in its proposed solution to the DND/CAF. Controlled Goods are defined in the Defence Production Act and the Controlled Goods List is contained in the Schedule (section 35) of the Act.

If Controlled Goods are used in the proposed solution, participants must identify and confirm that they are registered in the Controlled Goods Program with Public Services and Procurement Canada (PSPC) or are excluded or exempt from registration in the Controlled Goods Program with an explanation therefor. Visit the Controlled Goods Program website for more information.

Insurance

''The contractor must obtain Commercial General Liability Insurance and maintain it in force throughout the duration of the Contract, in an amount usual for a contract of this nature, but for not less than $10,000,000 per accident or occurrence and in the annual aggregate.''

Options to determine applicable limits of insurance being requested when applying the Treasury Board Policy on Limiting Contractor's Liability in Crown Procurement Contracts are:

A. In all cases for limitations of liability **equal to or less than $2 million,** CGL insurance required of contractors shall be a minimum of $2 million per accident or occurrence.

B. In all cases for limitations of liability **greater than $2 million but less than or equal to $10 million**, CGL insurance required of contractors shall be a minimum of $5 million per accident or occurrence.

C. In all cases for limitations of liability **greater than $10 million but less than or equal to $20 million,** CGL insurance required of contractors shall be a minimum of $10 million per accident or occurrence.

In all cases where limitations of liability **exceed $20 million,** refer to Risk Management Advisory Services.

Liability

The participant is liable for any damage caused by the participant, its employees, subcontractors, or agents to Canada or any third party. Canada is liable for any damage caused by Canada, its employees or agents to the participant or any third party. Canada and the participant agree that no limitation of liability or indemnity provision applies to this CFA unless it is specifically incorporated in full text in this CFA. Damage includes any injury to persons (including injury resulting in death) or loss of or damage to property (including real property) caused because of or during the performance of the Sandbox. DND/CAF has no responsibility for maintenance, repair, loss, or damage to any participant's materiel or equipment during or because of the Sandbox. Subject to Section 0, participants are fully responsible for insuring their own personnel, equipment, and activities at their discretion.

Language

Responses and consultations are to be provided in one of the two official languages of Canada (English or French).

Additional notes to applicants

Access to Information: All applicant consultations are documented, and this information is subject to the Access to Information Act. Applicants should identify any submitted information that is to be considered as either company confidential or proprietary. DND/CAF will not reveal any designated confidential or proprietary information to public and/or third parties, except for independent consultant(s) who may participate in the CFA process.

Participants will be asked to fill out the IDEaS Photo and Video Release Form for Individuals and the IDEaS Photo and Video Release Form for Entities before the start of their Sandbox participation.

IDEaS Program Surveys: As a condition of the program, participants are required to respond to short surveys from IDEaS for up to two years following the completion of the Sandbox event. The results of the surveys will feed into the measurement of performance indicators through the reporting requirements of the IDEaS program.

Public Affairs / Communication notification: The Government of Canada retains the right to make primary Sandbox announcements. Canada and the participant shall consult with each other, after the Sandbox selection, about all proposed news releases or public announcements relating to the Sandbox. This is to provide all parties sufficient notice of key Sandbox communications, and, where appropriate, the time to determine a course of action (including a mutually agreed date and location), line up representatives and prepare joint material. Notwithstanding the advance notice requirement, consent shall not be unreasonably withheld by either Party if a news release or public announcement must be issued in less than 15 working days as the result of unforeseeable circumstances, including matters of public safety or where an emergency response is required.

Enquiries

All enquiries and other communications related to this CFA must be directed exclusively to the CFA authority identified in the following section.

CFA authority
Tom Hughes
Manager – Innovation Exploitation
Department of National Defence, Defence Research and Development Canada
Innovation for Defence Excellence and Security Program (IDEaS)
Email: IDEaSSandboxes-EnvironnementsprotegesIDEeS@forces.gc.ca

Annex A – CUAS 2026 Sandbox Challenge

Disclaimer: Challenge requirements vs end-state operational requirements. Please note that the descriptions, characteristics, and criteria used for this challenge represent the limitations and desired characteristics to prioritize and select the IDEaS accepted solutions for the sandbox. They do not represent final operational requirements for any current or future procurement program.

CHALLENGE STATEMENT

The DND/CAF and its defence and security partners (RCMP, Public Safety, etc.) are seeking CUAS solutions that can detect and/or defeat Micro and Mini UAS with systems that can be integrated into the broader military command and control systems.

1. Background and context

1.1. The UAS landscape is rapidly evolving. The rapid increase of availability, affordability, complexity, and capabilities of UAS systems is posing increasing threats to the DND/CAF and our Defence and Security partners. Potential adversaries are also adapting UAS designs to evade current CUAS capabilities, by reducing the UAS visibility, minimizing radio-frequency emissions, increasing autonomy, operating at higher velocities, etc., thus rendering the current CUAS approaches obsolete. Proposed solutions to this challenge should consider not only what is available and a threat today, but also emerging UAS and CUAS capabilities and how they might be detected, defeated, and/or exploited tomorrow.

1.2. CUAS was identified as one of the priorities in Canada's 2017 defence policy *Strong, Secure, Engaged (*SSE) which stated: "*As the development of remotely piloted systems increases… Canada will require the appropriate capabilities to identify and defend against these burgeoning threats*" (page 73).

1.3. Due to the importance of this challenge, the CAF is in the process of establishing a strategic level Joint CUAS Office (JCO) for coordinating with the Canadian Army (CA), Royal Canadian Navy (RCN), Royal Canadian Air Force (RCAF), Canadian Special Operations Forces Command (CANSOFCOM), and our allies and partners. The information presented in this IDEaS CUAS challenge represents a blending of characteristics of interest to one or more of the services, as well as the RCMP.

1.4. The RCMP has an enduring responsibility for protecting Canadians from threats in a domestic environment, including security at major events such as the G7, Olympics, and VIP protection, including CUAS. The RCMP also works with their international security partners including assorted technology test and demonstration events.

1.5. The following CAF projects have a direct interest in CUAS systems and the results of this challenge:

1.5.1 **Canadian Forces Land Electronic Warfare Modernization (CFLEWM)**. CFLEWM is upgrading the Army's Mobile Electronic Warfare Teams in Light and Armoured platforms. While dedicated CUAS capabilities are out of scope for CFLEWM, a beneficial outcome would be to understand how multi-role EW

Sense and Attack capabilities can contribute to the CUAS fight, and how dedicated CUAS sensors could be integrated into the EW sensor network.

1.5.2 **Land Intelligence, Surveillance and Reconnaissance Modernization (Land ISR Mod).** Land ISR Mod is investigating capabilities that can provide sensor systems for the purposes of targeting. This project is mandated under SSE: Canada's Defence Policy – Initiative #42 and is funded. This project is in Options Analysis transitioning to Definition.

1.5.3 **Counter Uncrewed Aerial Systems (CUAS).** A specific CUAS initiative is investigating CUAS systems capable of defending critical infrastructure, vehicles, and personnel from micro and mini UAS. This project is not funded at this time, and consequently an intended date for any future procurement cannot yet be stated.

1.6. **UAS sizes to be considered for the challenge:** Micro and Mini UAS. For the purposes of this challenge, the following definitions are used:

1.6.1 **Micro UAS** with typical characteristics of:

- <2kg.
- up to 200ft Above Ground Level (AGL).
- normal mission radius of 5km Line of Sight (LOS).
- operating at high speeds up to 200 kph.

1.6.2 **Mini UAS** with typical characteristics of:

- 2-15kg.
- up to 3000ft AGL.
- normal mission radius of 25km LOS.

operating at high speeds up to 200 kph.

1.7. **CUAS methodologies**. The general methodologies for achieving CUAS effects can be characterized as:

- **Active detection**, in which the CUAS system is transmitting a signal in order to detect the UAS (such as radar), which has the disadvantage of potentially revealing the location of the transmitter, depending on the technology used.
- **Passive detection**, which conceals our own position and relies on detecting the UAS from effects it generates (such as visual detection, electronic signatures, audible noise, etc.).
- **Soft-Kill neutralization**, using means such as radiofrequency effects or other methods to deter, disable, take over, or otherwise mitigate the UAS.

Hard-Kill neutralization, using ammunition, nets, entanglers, missiles, lasers, microwave devices, or other means to physically disable the UAS.

2. **CUAS challenge essential outcomes**. Aside from addressing the challenge in an overall sense, there are no specific detailed essential challenge outcomes at this time.

3. **CUAS desirable outcomes:** DND/CAF is open to receiving all types of solutions with variable outcomes that are not restricted to the following list; however, the desirable outcomes on this list are of particular interest and solutions that address these in whole or in part have an increased likelihood of being selected to attend CUAS 2026:

3.1. Operating Outcomes of Interest

3.1.1 Integration into an External Command and Control System.

- The UAS threat is only one threat amongst many that CAF must constantly consider in a layered operational environment. While a singular CUAS system may be quite capable, if its information and control cannot be integrated into a common command and control structure its functional utilization is diminished, requiring additional human resources to manually fill that gap, which reduces both efficiency and effectiveness of the system and the deployed force.
- It is desirable that proposed systems/sensors/technologies are interoperable/compatible with digital protocols already in use by the CAF. This will enable the seamless integration of new technologies, sharing critical digital information throughout every level of Command and Control (C2) systems and potential remote control of the technology. The CAF protocols in use include Joint Range Extension Application Protocol (JREAP-C) J-Series messages, Variable Message Format (VMF) K-Series messages, Cursor on Target (CoT) messages, Sensing for Asset Protection using Integrated Electronic Networked Technology (SAPIENT).

3.1.2 Systems that can operate in a contested electromagnetic environment where radio frequency noise, jamming, and loss of external communications links, navigation and timing signals can occur.

3.1.3 Systems that are difficult for the enemy to detect, such as technologies with low or no electro-magnetic emissions or are easily concealed from visual observation.

3.1.4 Systems that minimize collateral damage when used, especially in such operations as police security for public gatherings.

3.1.5 Systems that can be rapidly deployed from home base to locations across Canada and the world, and once on site being able to quickly pack and go to another tactical location within the same general area.

3.1.6 Detecting, tracking and defeating swarms of UAS.

3.1.7 Detecting, tracking, and defeating high speed maneuvering drones, especially First Person View (FPV) ones.

3.1.8 Detecting, tracking, and defeating tethered UAS, notably fibre-optic tethers up to 30 kilometers in length.

- Tethered drones use a physical tether that provides power, data, or both from a tether station located on the ground, to the drone.

- This is a growing threat in CUAS operations as such drones don’t rely on radio connections for control and data transmission which makes detection of their presence more difficult, and they cannot be defeated by electronic jamming. When very thin fibre optic tethers are used, the tether can be as long as 30 kilometres in length.
- To detect and defeat this new kind of threat, methods that rely on RF energy will be less effective but potentially the tether itself provides new opportunities for innovative techniques. In addition to detecting and defeating the actual drone, perhaps the tether itself can be detected with visual or other sensor types that detect emissions or some other disturbance from the tether? Perhaps the drone can be defeated with methods that sever the tether, either physically or virtually?

3.2. **Operational scenarios.** The UAS threats occur in a variety of operational scenarios, six of which are of specific interest to defend against. It is desirable that a solution addresses as many of these as possible, each to the maximum extent possible, in both day and night conditions:

3.2.1 **Operating base**. Defending a Forward Operating Base (FOB), airfield, or VIP conference location in which a CUAS system can be in a static location once deployed, and where equipment size and power consumption is not a major issue. The perimeter of the area to be defended is a circle with a 2.5 km radius. The combined location and quantity of the systems used must be located within that circle with an effective range extending beyond that perimeter in all directions to prevent the UAS from approaching the perimeter. The capability to distinguish authorized and non-authorized aircraft, drones, and other objects in the airspace is relevant.

3.2.2 **Mobile vehicle**. Defending a mobile vehicle force element such as a patrol of five vehicles, in which the CUAS system must be vehicle-mounted and powered for mobility, creating a defensive bubble around the vehicles while on the move.

3.2.3 **Dismounted personnel**. Defending a small element of 12 dismounted soldiers or a VIP group in an isolated location, in which case the CUAS system and its power source must be “Person Portable”. Ideally also operating while the group is on the move, creating a defensive bubble around the group.

3.2.4 **Urban environment**. Operating in urban scenarios such as complex and cluttered infrastructure, obstacles, and electromagnetic environments. The area to be defended is a major city downtown location and a square of 4 x 4 city blocks, with office towers up to 10 stories high on some or all of the blocks to be defended.

3.2.5 **Naval environment**. Defending an RCN frigate sized ship that is (i) underway in littoral waters that vary from large straits to confined entries to harbours; and (ii) alongside a dock or anchored in a harbour. The equipment will have to contend with obstacles such as the ship's superstructure, the unique electromagnetic environment surrounding the ship, the various speeds and movements of a ship, a variety of coastal, urban, and port landscapes, and it will have to withstand prolonged exposure to the marine salt environment.

3.2.6 **Monitoring and defending a linear border**. Such borders are relevant to military front lines of combat and to geo-political boundaries and can be many kilometres in length. For the purposes of relative resource and capability comparisons amongst different solutions, for any one system, how many are required at what spacing to provide a CUAS capability along a 10-kilometer straight line border?

4. **Technology Areas of Interest**. DND/CAF is open to receiving all types of solutions, however technologies and concepts that are new, different, and have an unknown future potential will be of higher interest relative to technologies and concepts that are largely duplicating other existing similar solutions.

4.1. For CUAS 2026 in Suffield, selection emphasis in the following technology areas can be expected provided their performance is relevant. Even if these technology areas are previously known, improvements in these areas are of interest:

4.1.1 Interceptors.

4.1.2 Hard-kill solutions, particularly proximity munitions, and directed energy such as lasers and microwaves.

4.1.3 Beyond line-of-sight capability.

4.1.4 Networks of low-cost sensors.

4.2. For CUAS 2026 in Suffield, selection in the following areas is less likely as these methods have been seen before; however, selection can still occur, especially if substantive improvements over current such systems are evident.

4.2.1 Detect:

- Radar
- Acoustic
- RF Signal
- Optical

4.2.2 Defeat:

- RF Jamming and Cyber
- Nets
- Small arms ballistic projectiles

5. **Detect and defeat solution characteristics and state of the art**.

5.1. To assess any specific solution's ability to address the CUAS challenge, a description of any proposed solution is required. This is done by a series of questions and short answers in the Application Form to explore relevant characteristics of any CUAS system. Proscribing this method ensures that a common solution description structure is used for all solutions, regardless of the company or technology type.

5.2. The questions posed are explained in the application form and are a combination of the preceding desirable outcomes and operational scenarios, as well as the tables below for a variety of other descriptive characteristics:

5.2.1 There is a one table for the characteristics applicable to Detect technologies, and a separate table for the Defeat characteristics. Many are similar between the two but are replicated for completeness in each.

5.2.2 The comments column gives a short description of the current state of the art on that topic, and where applicable an indication of what types of improvements in that topic would be of interest to Canada.

5.3. Solutions seeking to attend the CUAS Sandbox 2026 should be at similar or higher levels than comments provided in these tables, or collectively do more of these characteristics at similar or higher levels but within a single solution.

Key message:

- Use the CUAS Application Form to submit your full information package.
- These two tables provide some supplemental information on many of the characteristics used in the form.

Table 1: CUAS Detect Characteristics

Detect characteristic	Description	Comments
Types of drones detected	☐ Rotary drone ☐ Fixed wing drone ☐ RF controlled ☐ RF Silent ☐ LTE/5G ☐ Tethered drones	Most types are detected, but not always in a single solution. Improved flexibility in RF frequency and/or cellular RF frequency detection is desired. Current systems can detect larger UAS easily at long-range but are challenged by UAS in the sub-250-gram category because of their low radar cross-section and low visible and infrared signature. Future systems will need to address these smaller threats while simultaneously reducing the false alarms and clutter produced by similar targets in the environment such as birds.

Detect characteristic	Description	Comments
	Tethered drones use a physical tether that provides power, data, or both from a tether station located on the ground, to the drone. This is a growing threat in CUAS operations as such drones don’t rely on radio connections for control and data transmission which makes detection of their presence more difficult, and they cannot be defeated by electronic jamming. When very thin fibre optic tethers are used, the tether can be as long as 30 kilometres in length. To detect and defeat this new kind of threat, methods that rely on RF energy will be less effective but potentially the tether itself provides new opportunities for innovative techniques. In addition to detecting and defeating the drone with more traditional methods, perhaps the tether itself can be detected with visual or other sensor types that detect emissions or some other disturbance from the tether? Perhaps the drone can be defeated with methods that sever the tether, either physically or virtually?	
Operating conditions	☐ Daytime ☐ Nighttime ☐ Rain ☐ Fog ☐ Falling snow ☐ The target is in or behind cloud cover	Some solutions can already detect in all weather and day/night conditions. Many current systems are not operational in adverse weather conditions such as heavy rain and snow. As UAS capabilities evolve, these restrictions will need to be overcome.
Detection range	This is the detection range for your solution.	To provide acceptable early warning, detection, tracking, and identification at ranges substantially greater than 3 km should be achievable.
Arc of coverage - horizontal	☐ 0 - 44 degrees ☐ 45 - 89 degrees ☐ 90 - 180 degrees ☐ > 180 degrees	360-degree coverage, even if multiple systems are integrated, is readily achievable.
Arc of coverage - Vertical	☐ 0 - 29 degrees ☐ 30 - 59 degrees ☐ 90 - 180 degrees ☐ 60 - 90 degrees	Fully vertical coverage remains a challenge, in particular the ability to detect UAS operating near the ground or at high altitudes. Current systems are mostly composed of expensive, point sensor systems. In order to provide greater protection, future systems will need to cover much larger areas with lower cost, distributed sensors networked together.

Detect characteristic	Description	Comments
Passive detection	The solution uses techniques to locate the UAS threat such that the use of its systems is not detectable by the enemy, and consequently our use of the solution does not reveal our location to the enemy. This describes all emissions or other potentially detectable aspects of your solution.	Many current passive systems rely on radiofrequency detection of UAS signals. For future UAS that do not emit RF signals, other means of passive detection will need to be developed. Current optical detection methodologies do not provide adequate range.
Recognize the class of a UAV	Recognition of the broad class of an object's type.	Other than RF recognition/identification, automated systems are not yet adequately reliable or long-range.
Identify a UAS	Identifies to specifically determine details about the object detected and differentiate between types of mini/micro UAS.	Other than RF recognition/identification, automated systems are not yet adequately reliable or long-range.
Detection and tracking of swarms.	Capability to detect swarms (3 or more threat UAS) and track each individual threat UAS within the swarm.	Current systems capable of tracking multiple UAS generally do not provide adequate situational awareness. Recognition and identification systems often operate at ranges that are too short or are too slow to sequentially identify multiple UAS.
Friend/Foe discrimination	The capability to have a friend/foe discrimination capability.	Future airspaces will be a complex mix of friendly and enemy UAS which will require quick accurate discrimination between friend and foe UAS.
Detection and tracking of high-speed manoeuvring targets, such as First Person View (FPV) drones	0 - 10 km/hr 11 - 50 km/hr 51 - 100 km/hr 101 - 150 km/hr 151 - 200 km/hr >200 km/hr	The prevalence of FPV drones in the battlespace means that CUAS solutions must be able to deal with drones that are changing speed and direction rapidly.
Locate the UAS's ground control station	The capability to locate the enemy UAS ground control station.	Current systems require tens of seconds to detect and alert operators to the presence of UAS. With decreasing size and increasing speed, this does not leave adequate response time for countermeasures.
Speed of solution response	The time in which a CUAS system can respond is an important measure of the system's functional effectiveness in an operational environment.	Quicker mitigation is important to ensure target stand-off from the area to be protected.

Table 2: CUAS Defeat Characteristics

Defeat characteristic	Description	Comments
Types of drones defeated	☐ Rotary drone ☐ Fixed wing drone ☐ RF controlled ☐ RF Silent ☐ LTE/5G ☐ ☐ Tethered drones.	Current systems can defeat larger UAS at short-range but are challenged by UAS in the sub-250-gram category because of their low physical cross-section and maneuverability. Future systems will need to address these smaller systems.
	Tethered drones use a physical tether that provides power, data, or both from a tether station located on the ground, to the drone. This is a growing threat in CUAS operations as such drones don’t rely on radio connections for control and data transmission which makes detection of their presence more difficult, and they cannot be defeated by electronic jamming. When very thin fibre optic tethers are used, the tether can be as long as 30 kilometres in length. To detect and defeat this new kind of threat, methods that rely on RF energy will be less effective but potentially the tether itself provides new opportunities for innovative techniques. In addition to detecting and defeating the drone with more traditional methods, perhaps the tether itself can be detected with visual or other sensor types that detect emissions or some other disturbance from the tether? Perhaps the drone can be defeated with methods that sever the tether, either physically or virtually?	
Operating conditions	☐ Daytime ☐ Nighttime ☐ Rain ☐ Fog ☐ Falling snow ☐ The target is in or behind cloud cover	Many current systems are not operational in adverse weather conditions such as heavy rain, snow, and high winds. As UAS capabilities evolve, these restrictions will need to be overcome.
Effective range	This is the effective range for your solution in this scenario.	Higher speed UAS with longer-range sensors will require CUAS systems (other than RF jamming and takeover solutions) to engage and defeat at ranges substantially greater than 500m.
Functional without operator line of sight	The capability of the solution to continue and complete the defeat of the targeted UAS without requiring the operator to maintain their line of sight to either the solution or the target.	Current CUAS systems require operator line of sight to defeat UAS effectively.

Defeat characteristic	Description	Comments
Defeat a specific UAS	The capability to select and defeat a specific drone from amongst the clutter of multiple drones.	With an operating environment involving friendly and enemy UAS, defeat systems will need to be selective about which UAS they are targeting.
Defeat swarms of UAS	The capability to defeat swarms of UAS.	Current hard-kill defeat systems operate in a sequential manner defeating one UAS at a time. As UAS become more numerous, the rapid defeat of multiple UAS will be desirable.
Defeating high-speed manoeuvring targets, such as First Person View (FPV) drones	□ 0 - 10 km/hr □ 11 - 50 km/hr □ 51 - 100 km/hr □ 101 - 150 km/hr □ 151 - 200 km/hr □ >200 km/hr The prevalence of FPV drones in the battlespace means that CUAS solutions must be able to deal with drones that are changing speed and direction rapidly.	Current hard-kill defeat solutions have trouble engaging small, agile, and fast targets such as FPVs.
Defeat the target's ground control station	The capability to target and defeat the GCS.	Current systems that can defeat the enemy controller rely on adequate RF line-of-sight and RF signal strength to a ground-based receiver. At the same time, ranges for UAS RF signal controls are increasing providing longer operator standoff from target. Novel methods will be required to quickly defeat control stations at long-range.
Speed of solution response	The time required for a CUAS system to respond is an important measure of the system's functional effectiveness in an operational environment.	Quicker mitigation is important to ensure target stand-off from the area to be protected.
Exploiting the data from the target UAS	The capability to capture the data from the target UAS through either (i) a cyber means; or (ii) by enabling the physical recovery of the target UAS itself, without destroying the target.	Current systems can capture and acquire data from only a select few UAS systems (specific RF signals, or slow-moving UAS capture). This capability should be expanded.

Annex B – CUAS evaluation of scientific and technical risk

In seeking innovative solutions, the IDEaS program is open to high-risk untested solutions, provided such solutions come with reasonable substantiation and a high impact to addressing the challenge at hand. High risk without high reward is of less interest.

This full process is only undertaken for a specific solution when the selection decision is in doubt due to the risk. To enable that aspect of the selection process, the following risk assessment profile is used as an overall assessment of the technical feasibility and risk of the solution successfully performing to the extent described by the applicant.

Consequently, it is the quality and completeness of the applicant's responses throughout their application that provide the applicant's opportunity to influence the risk assessment. Incomplete or unreasonable explanations will tend to increase the risk level.

The risk assessment reflects a combined consideration of:

1. What has already been proven through testing? Were the solution's levels of performance and characteristics successfully tested to substantiate the description? To emphasize, untested does not mean unacceptable, and it is fully expected that concepts and prototypes will be untested in many areas.
2. If not tested, how reasonable were the provided substantiations for the claimed yet untested descriptions?
3. From a technical perspective and given those substantiations, what is the resultant likelihood for the solution not achieving its described performance levels or characteristics?
4. What would be the consequence to the solution's effectiveness be in addressing the challenge, if that likelihood occurs?
5. With that likelihood and consequence, what is the overall scientific and technical risk?

The risk evaluation is based on the information provided throughout the application process. No additional specific risk information is provided by the applicant. There is no point score for this risk assessment. Instead, the results are used during the strategic selection process, as described in the Applicant Guide.

<u>Risk evaluation process:</u>

Question 1: Testing to date. How often were the described levels of performance and characteristics supported by successful and repeatable testing?

- Fully untested
- Mostly untested
- Mixed tested and untested
- Mostly tested
- Fully tested

Question 2: How reasonable was the provided substantiation to support the described level of performance or characteristic when testing was not yet done, not successful, or not repeatable?

- **Extremely unreasonable.** Substantiations were almost always unreasonable or not present, based on unproven or untested principles that do not align, or even contravene, known science and technology principles.
- **Mostly unreasonable.** Substantiations were usually unreasonable or not present, and while not fully misaligning or contravening known science and technology principles did not provide an adequate explanation as to why that outcome would be possible.
- **Generally reasonable.** Substantiations were generally reasonable and present, generally remaining within touch of the boundaries of accepted science and technology principles, even if stretching those boundaries to a reasonable extent.
- **Mostly reasonable.** Substantiations were often reasonable and present, generally remaining within the boundaries of accepted science and technology principles.
- **Extremely reasonable.** Substantiations were almost always reasonable, based on principles that are well understood and accepted using well established science and technology principles.

Risk table 1:
Resultant likelihood of not achieving the described performance and characteristics.
Derived from the intersection of the preceding Question 1 and 2.

From Question 2 **Reasonableness of substantiation for untested characteristics**	**Extremely unreasonable**	Moderate	Moderate	High	Extreme	Extreme
	Mostly unreasonable	Low	Moderate	High	High	Extreme
	Generally reasonable	Low	Moderate	Moderate	High	High
	Mostly reasonable	Negligible	Low	Moderate	Moderate	High
	Extremely reasonable	Negligible	Negligible	Low	Moderate	Moderate
		Fully tested	**Mostly tested**	**Mixed**	**Mostly untested**	**Fully untested**
		From question 1: Testing to date				

Enter the resultant "Likelihood" from Table 1 into "Table 2: Resultant risk" below.

Question 3: Consequence. For those performance levels or characteristics that were less likely to be achieved, what would be the collective consequence to the solution's effectiveness in the operational scenarios if they are not achieved?

- **Extreme.** The inability to achieve those levels would collectively and significantly impede the solution's overall claimed operational scenario effectiveness, to the point of it losing applicability to the challenge.

- **High.** The inability to achieve those levels would collectively and significantly impede the solution's overall claimed operational scenario effectiveness, to the point of it losing applicability to the one or more of the claimed scenarios.

- **Medium.** The inability to achieve those levels would collectively degrade the solution's overall claimed operational scenario effectiveness, but it would still have some applicability to some of the claimed scenarios.

- **Low.** The inability to achieve that those levels would collectively have minimal impact to the solution's overall claimed operational scenario effectiveness.

- **Negligible**. The inability to achieve that those levels would collectively have virtually no impact to the solution's overall claimed operational scenario effectiveness.

Resultant risk table 2
Derived from the intersection of the Likelihood from Table 1 and the consequence from question 3:

Consequence from question 3	**Extreme**	Significant	Major	High	Severe	Severe
	High	Moderate	Significant	Major	High	Severe
	Medium	Low	Moderate	Significant	Major	High
	Low	Negligible	Low	Moderate	Significant	Major
	Negligible	Negligible	Negligible	Low	Moderate	Significant
		Negligible	**Low**	**Moderate**	**High**	**Extreme**
		From Risk table 1 above: Likelihood				

The result from Table 2 is the overall assessment of a solution's "Scientific and technical risk".

Annex C – CUAS 2026 Sandbox “Diamond in the Rough” prizes

Introduction

The Diamond in the Rough (DIR) prizes are awarded for CUAS innovations demonstrated at the Sandbox that have impact in the field of CUAS and are tracking towards success with good growth potential and ability to address their demonstrated limitations, and a result receive financial non-repayable grants with up to $1,750,000 in total prizes available.

Creating a true CUAS capability can involve a mix of technologies and capability levels with a collective layered approach for CUAS defence rather than a single individual system being “the best and only”. As the Sandbox will include such a mix of technologies and capabilities, the awarding of prizes is not as simple as who detected the most targets, or shot down the most, or did it at the longest range, etc.

Instead, the Diamond in the Rough prizes are being awarded within the context of seeking whose CUAS innovation is tracking towards success, even if not quite there yet. Are they best filling a niche of CUAS with good potential for growing? Are the current limitations of the technology understood, and can further development expand the technology beyond those limitations?

Consequently, the process, criteria, and prizes are designed to identify and reward innovators who have:

1. Created a solution of interest to CAF, such that they were selected to attend the Sandbox; and
2. Demonstrated the performance of their solution at the Sandbox; and
3. Will have impact in the field of CUAS; and
4. Attempted test profiles at the sandbox beyond their solution’s capabilities to the point of failure, such that current limitations are demonstrated; and
5. Have the potential for further improvement to address those demonstrated limitations as their solution’s technology approach has not yet plateaued and the company has a plan and the capacity to conduct the work; and
6. Have created a continuing post-Sandbox interest from the CAF in their approach to CUAS as determined by examining all the information from the original Sandbox application to the observations and results at the sandbox; and
7. Utilizing the Strategic Selection Parameters are thus worthy of investment from IDEaS via a Diamond in the Rough financial grant.

With consideration to the potential and impact, prizes will be awarded for up to the following notional amounts. Final prize amounts will be established to align with the developmental potential of the selected technologies:

1st Place	up to $1,000,000
2nd Place	up to $500,000
3rd Place	up to $250,000

Prize decisions by the CUAS Committee are considered final. There is no appeal process.

Eligibility

Eligibility for the DIR prizes is a post-selection pre-sandbox process. Innovators that are not eligible for the DIR prizes, or choose to not participate in its additional prize process, are still fully welcome to participate in the sandbox without being eligible for the DIR prizes.

To be eligible to receive a DIR prize the innovator must meet all of the following:

1. Be selected to attend the sandbox;
2. Be a legal entity duly incorporated and validly existing in Canada prior to the first day of the sandbox.
    a. International applicants may be eligible, provided they meet this requirement with a legal entity duly incorporated and validly existing in Canada.
    b. For international or Canadian companies not incorporated in Canada at the time of your original sandbox application it is a process that can be completed in the time between selection and commencement of the sandbox provided you don’t delay in doing so. These websites may be of assistance:
        i. Starting a business - Canada.ca
        ii. Registering your business with the government - Canada.ca
        iii. Opening a Canadian bank account for non-Canadians - Canada.ca
    c. Examples of acceptable legal entities duly incorporated and validly existing in Canada, include:
        i. Canadian universities and educational institutions chartered in Canada.
        ii. Incorporated Canadian not-for-profit organizations or associations.
        iii. Incorporated Canadian for-profit companies, organizations or associations.
        iv. Provincial/territorial, or municipal government organizations.
3. The following are not eligible regardless of any other status:
    a. Federal and provincial crown corporations are not eligible.
    b. Government entities at any level of any country other than Canada.

4. Submit their DIR application by the date indicated by the Sandbox team, notionally one month prior to the commencement of the sandbox.

5. The participant must conduct actual demonstrations at the Sandbox. If no demonstrations are conducted, they are not eligible, regardless of cause unless excepted as described under the “Extenuating circumstances that impact demonstration conditions and outcomes” section below.

The evaluation and selection of the winners will be a staged process consisting of:

Stage 1: Initial Sandbox application.

- Application, evaluation and selection to attend the CUAS 2024 Sandbox, as described throughout this Applicant Guide.
- Only those applicants selected to attend the Sandbox proceed to Stage 2.

Stage 2: Pre-Sandbox, DIR application

- Prior to the Sandbox all participants will be given the opportunity to apply and agree at their discretion to participate in the DIR prizes.

- This will include a short DIR application template document for the participants to respond to the criteria in the table below that will be used during the DIR process.
- This template will be available to the Sandbox participants after they are selected and is to be submitted approximately one month prior to the Sandbox. A precise date will be communicated by IDEaS in advance of that.

Stage 3: Demonstrations and evaluations at CUAS 2024

- Demonstrations at the Sandbox will be evaluated by Sandbox observer teams.
- All Sandbox participants that applied to participate in the prizes will be evaluated against all Diamond in the Rough criteria as described below.
- Evaluators will consider all information provided during the original application and evaluation process as well as the specific DIR Application information and the evaluations at the Sandbox.
- Those evaluated as a "Pass" against all mandatory criteria will proceed to Stage 4.

Stage 4: Selection of the DIR prize winners

- Awarding of the prizes from those that proceeded to Stage 4 will be made using the Strategic Selection Parameters as described in the original Sandbox selection process in this Guide, inclusive of consideration of:
  - the evaluation results from the DIR criteria described below.
  - all other information provided during the entirety of the Sandbox process, including the original application and evaluation; and
  - the Strategic Selection Parameters.
- In the event that there is a tie outcome for any of the prize positions that cannot be suitably broken using the strategic parameters, the CUAS Committee may choose to divide the cumulative prize for such tied positions equally. For example, if 1st place and 2nd place remain tied, each may be declared as tied for first place with each receiving half of the sum of the 1st and 2nd place prizes. The 3rd place prize and the total prize money awarded remain unchanged in this example.
- The selection process and announcements of winners will be made as soon as possible after the conclusion of the Sandbox.
- Prize decisions by the CUAS Committee are considered final. There is no appeal process.

CUAS 2026 Sandbox DIR evaluation and criteria

The following table provides the criteria that will be used for the DIR evaluation.

1. **Criteria design**. The criteria are designed to equitably accommodate a wide range of technology types and operational applications across different layers of the CUAS spectrum and at different TRLs. It cannot be as simple as "who has the longest range" as doing so would not be equitable to technology types designed for the short-range layer of CUAS defense, or those only designed for detecting and not defeating UAS, etc. Consequently, the criteria are broad based rather than just specific performance areas and numbers.

2. **Extenuating circumstances that impact demonstration conditions and outcomes**.

   a. Variations in weather conditions and other factors outside of the innovator's control can influence the demonstrations conducted at the Sandbox. It would be unfair to compare one innovator's performance in ideal conditions, against another who experienced more challenging conditions as they were at the Sandbox during a different week with substantively different and impactful conditions (high winds or heavy rain for example).

   b. To account for this, where applicable, possible, and reasonable, the evaluations of the criteria for each innovator may include allowances for such factors to the extent possible to enable an equitable evaluation of all participants, and only if such factors:

      i. Would make an appreciable difference to the evaluation; and
      ii. Were outside the responsibility and control of the participant. Typically, these will be restricted to the environmental conditions, or variations in the Red Team of targets available. Issues such as solution reliability or design would not typically be included, nor would the inability to demonstrate something due to an equipment shipping issue or other administrative/logistical factor caused by the participant or an agent or contractor engaged by them.

   c. The decision to apply or not apply any such evaluation allowances is at the sole discretion of Canada.

3. **Criteria scoring**.
   a. Each mandatory criteria is evaluated as a Pass/Fail.
   b. Each point rated criteria is scored on a scale of 0-100 as described in its criteria description.
   c. Note that during the final selection of the DIR prize recipients, selections will consider the cumulative score and scoring on individual criteria.

CUAS 2026 Sandbox DIR mandatory criteria

After being selected, Sandbox participants submit a DIR application form of approximately 4-6 pages in order to provide responses for these criteria.

Mandatory criteria	Description and scoring
MC-1 Eligibility – Business status Prior to commencement of the Sandbox on May 27, 2024, eligible recipients of prizes must be a legal entity duly incorporated and validly existing in Canada. This need not be in place at the time of Sandbox application in October 2023.	**PASS**: The innovator has provided proof prior to arrival at the Sandbox of at least one of: • Canadian universities and educational institutions chartered in Canada. • Incorporated Canadian not-for-profit organizations or associations. • Incorporated Canadian for-profit companies, organizations, or associations. • Provincial/territorial, or municipal government organizations. • International applicants may be eligible, provided they meet this requirement with a legal entity duly incorporated and validly existing in Canada. **FAIL**: The innovator has not provided proof of at least one of the above list. The following may be of assistance: • Opening a Canadian bank account for non-Canadians - Canada.ca • Starting a business - Canada.ca • Registering your business with the government - Canada.ca
MC-2 Eligibility – Demonstrations were conducted at the CUAS 2024 Sandbox The conduct of a demonstration does not mean that the demonstration was successful in itself, it just means the demonstration was conducted.	**PASS**: • Sufficient demonstrations were given to enable a reasonable evaluation of the solution. **FAIL**: • Insufficient demonstrations were given to enable a reasonable evaluation of the solution; and • There were insufficient circumstances to enable a projected evaluation, as described above in the preceding section “Extenuating circumstances that impact demonstration conditions and outcomes.”

CUAS 2026 Sandbox DIR Point Rated Criteria (PRC)

Note that when referring to “other solutions”, that includes all solutions known to Canada from any source. It is not only the other solutions at the Sandbox unless stated as such.

Point Rated Criteria	Description and scoring
PRC-1 Creating impact in the field of CUAS	To develop an assessment of the solution’s impact in the field of CUAS, evaluators will consider the following sub-criteria:

CUAS 2026 Sandbox DIR Point Rated Criteria (PRC)

Note that when referring to “other solutions”, that includes all solutions known to Canada from any source. It is not only the other solutions at the Sandbox unless stated as such.

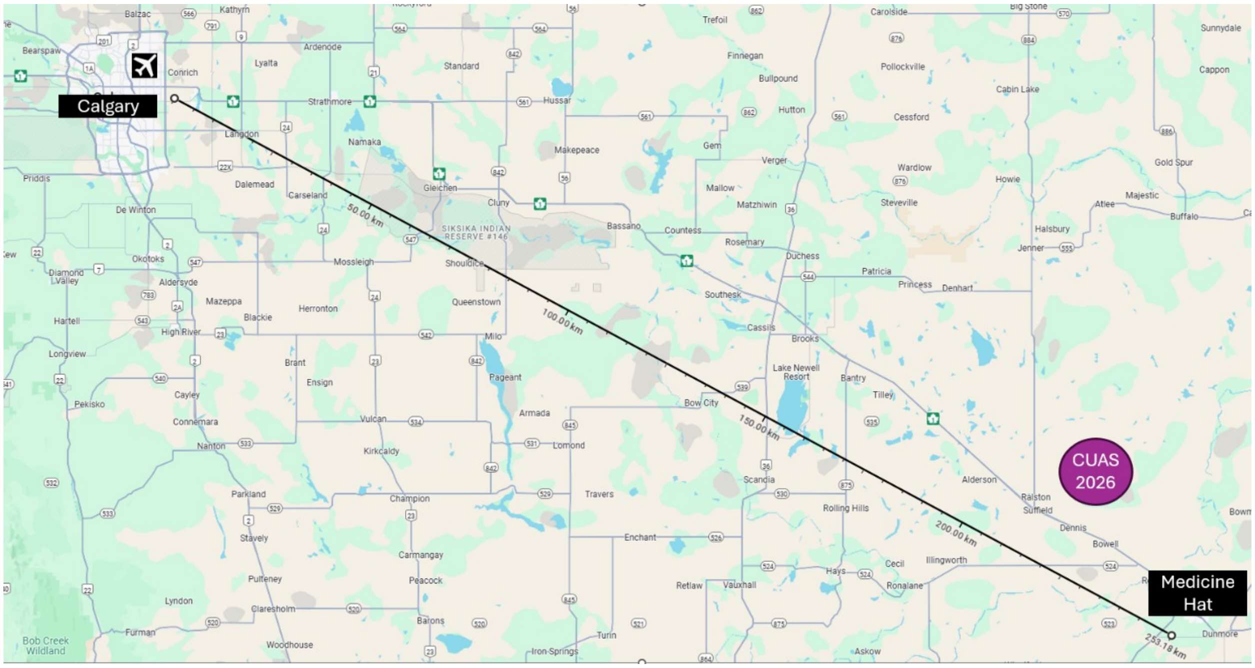
Point Rated Criteria	Description and scoring
PRC 1-1 **How unique is the solutions method?**	1. Multiple other solutions use the same method. (0 points) 2. Other solutions use similar methods, but there are some minor improvements to this solution. (25 points) 3. Other solutions use similar methods, but there is a major unique aspect to this solution. (50 points) 4. The solution is mostly unique, with some minor similarities to other solutions. 5. The solution is a first of its kind. (100 points)
PRC 1-2 **How well did it perform relative to what its method would be expected to achieve, and how advanced its TRL is?**	The TRL establishes the bar for where the current level of performance at the sandbox would be “expected” for a solution. If the TRL is lower, weaker performance is to be expected so a higher score can be given if the potential for improvement at higher TRLs seems evident. If the TRL is already higher, better performance is expected at the sandbox, so the scoring would reflect that. 1. Not particularly well. (0 points) 2. Somewhat well. (25 points) 3. Moderately well. (50 points) 4. Quite well. (75 points) 5. Extremely well. (100 points)
PRC 1-3 **Is it filling a gap in CUAS operations that other solutions are not adequately addressing?**	1. No. There are many other solutions already sufficiently meeting this operational effect. (0 points) 2. Somewhat. There are a few but not many solutions in the same space. This solution would only offer marginal improvements beyond what the other solutions already do. (25 points) 3. Partially. There are other solutions with similar operational effects, but the level of effectiveness is less than ideal and an additional solution working in this area is of good value. (50 points) 4. Mostly. There are a few other effective solutions in this space with some minor shortfalls that this solution seems to be capable of addressing. (75 points) 5. Yes. The solution is addressing a niche of CUAS that very few, if any, other solutions are sufficiently addressing. (100 points)

CUAS 2026 Sandbox DIR Point Rated Criteria (PRC) Note that when referring to “other solutions”, that includes all solutions known to Canada from any source. It is not only the other solutions at the Sandbox unless stated as such.	
Point Rated Criteria	**Description and scoring**
PRC-2 Demonstration of solution limitations DIR prizes are for funding technologies that with further investment and development can be substantively improved beyond current limitations. Evaluating that aspect requires demonstration of current limitations. If no limitations are shown and boundaries are not pushed and exceeded, the awarding of a DIR prize is in doubt.	For a DIR prize, the Innovator is expected to include test profiles that push their technologies beyond limits to the point of failure to adequately detect or defeat the target. Such “demonstrations to failure” could cover all the characteristics included in the sandbox application form; however, emphasis for this DIR evaluation will be on these “**capability areas**”: 1. Maximum effective ranges and altitudes. 2. Speed of response, detection, or time to kill. 3. Maximum speed of target and extent of target maneuverability. 4. Target types 5. Dealing with concurrent targets (swarms) **The evaluator will consider the collective demonstrations conducted and assess to what extent the limitations of the technology were demonstrated and understood:** **Scoring:** • **0 points – No understanding**. The demonstrations were fully within the capabilities of the solution. The solution seemed to be capable of doing better but the innovator was not demonstrating to the point of failure. We have no understanding of the solution’s limitations. • **25 points – Marginal understanding**. The demonstrations were mostly within the capabilities of the solution, but a few limitations were shown. The solution seemed to be capable of doing better in most areas. We have a marginal understanding of the solution’s limitations. • **50 points – Some understanding**. The capability areas were an even mix of demonstrated limitations, and limitations that were not reached. We have some understanding of the solution’s limitations. • **75 points – Good understanding**. The limitations of the solution were mostly demonstrated. We have a good understanding of the solution’s limitations. • **100 points – Excellent understanding**. The limitations of the solution were fully demonstrated to the point of failure. We have an excellent understanding of the solution’s limitations.

CUAS 2026 Sandbox DIR Point Rated Criteria (PRC) Note that when referring to “other solutions”, that includes all solutions known to Canada from any source. It is not only the other solutions at the Sandbox unless stated as such.	
Point Rated Criteria	**Description and scoring**
PRC-3 Two-year growth plan Typically, the life cycle for many solutions follows a developmental path with a slow start for initial iterations followed by a period of accelerating cycles of developments with major improvements or leaps in performance and production efficiency, culminating in a flattened plateau as the limits of that methodology are reached and further growth slows. DND/CAF is interested in solutions with a strong growth potential.	In relation to the state of the art for the technologies and methods used by the solution, describe your plan for the solution’s growth over the next two years commencing after the Sandbox (to September 2028), including: • An overview of the planned work. • Substantiation for, and by how much, its performance is reasonably expected to increase. • Expected TRL at September 2028. The described growth must be substantively different and an improvement. The evaluation will consider if the proposed growth of the solution is of interest and relevance to DND/CAF as follows: • **0 points -** Of negligible interest. • **25 points -** Of low interest. • **50 points -** Of moderate interest. • **75 points -** Of high interest. • **100 points -** Of extreme interest.
PRC-4 Capacity to execute the two-year plan.	Describe, explain, and substantiate the company’s capacity to execute the described two-year growth, including management, technical development, testing, and production. **Scoring**: • **0 points –** No reasonable explanation of such capacity was evident. • **25 points –** Some capacity was evident, but the substantiation was weak, lacking in sufficient specifics to give confidence the work could be achieved as described. • **50 points –** A reasonable capacity was evident, likely sufficient to meet the major objectives, but with some risk. • **75 points -** A reasonable capacity was evident, sufficient to meet major objectives with little capacity risk. • **100 points -** A fully reasonable and substantiated capacity was evident, sufficient to meet the major objectives and with capacity allowances included to accommodate unexpected issues.

Annex D – CFB Suffield and the Test Site

The Sandbox is located at Canadian Forces Base Suffield, Alberta, a 30-minute drive west of Medicine Hat which is the closest city for hotels. The closest international airport is in Calgary with a four-hour drive to Medicine Hat, or you can use a domestic flight to the Medicine Hat airport.



The CUAS Test Range in CFB Suffield.

The main test site from a drone's camera. There are two others...

While you are there you get a fully equipped test lane with dedicated covered work and storage spaces, electrical power and internet, isolated from other companies to protect your intellectual property.

We provide a Red Team of multiple target types and flight profiles. These are some of the targets used in 2024. Targets for 2026 will be adjusted to meet emerging threats and technologies at the Sandbox.