Safeguarding Australia Technology Challenges

2021

Information for Applicants

The National Security Science and Technology Centre (NSSTC) is calling for proposals from Australian businesses, universities and publicly funded research agencies seeking funds to support projects transitioning proof-of-concept and early prototype solutions to specific challenges through verification or integration.

About the Challenges

Three separate S&T challenges are being proposed which fall under the Investigative Support and Forensic Science (ISFS) priority area. The challenges are aimed at Technology Readiness Level (TRL) 5-7, with proposed solutions seeking to provide maximum impact to national security agencies. They will support the further development of mature research solutions (which have reached or surpassed proof of concept stage) through to a leading edge prototype solution.

Up to $200,000 (ex GST) per project is available to support a maximum of three projects of up to 18-24 months' duration. While the expectation is that one project will be funded in each challenge area, this will be dependent on the quality and relevance of the submissions received. DSTG reserves the right to fund projects in any one, two or all three of the challenges. DSTG also reserves the right to not fund any projects if no proposals of sufficient quality are received.

Challenge 1: Safe Vehicle Interdiction

Use Case: Over the last decade there has been an increase in the use of vehicles as weapons to cause harm and damage to persons and property within our communities. We have witnessed the devastation this can cause during international incidents such as the 2016 Nice truck attack, and closer to home, with two occurrences in the Melbourne CBD during 2017. Law enforcement are continually seeking to add to their available tools, improving their capability to effectively de-escalate such high-risk situations and minimise harm.

Challenge: to have single or multiple capabilities that will allow police officers to quickly slow down and render inoperable a vehicle in a no notice scenario where a vehicle (to include motor vehicles and trucks of all ages) must be stopped prior to reaching a targeted destination – while minimising collateral damage to persons and infrastructure in close proximity of the targeted vehicle.

Requirements: Activation of the capability will need to be responsive, deployed with minimal notice or pre-planned.

The capability will need to be:

a. Remotely deployed and activated (ie a portable capability that can be deployed/activated/deactivated remotely to a target vehicle),
b. Deployed by an operator within a separate vehicle (ie be man portable and operated by a single individual even whilst driving),
c. Able to be deployed and operated from a device mounted on or used from within a vehicle, or;
d. Able to be deployed and operated from an aerial vehicle such as an autonomous drone;
e. Agnostic to any target vehicle or truck: size, age (with and without electronic management systems); and

f. Be deployable from a distance of 10 m or more and in ideal cases from a further safe distance (100m +) to ensure protection of law enforcement officers and members of the public.

If a device requires physical contact with a target vehicle to be effective the device will have to be able to be activated/deactivated quickly in order to minimize collateral damage and ensure police officer safety.

Challenge 2: Enhanced Crime Scene DNA Collection

Use case: Current and emerging DNA techniques offer an ever-increasing level of discriminating power in addition to their ability to provide results on trace quantities of material. With this comes a greater need to ensure protocols, procedures and materials used during sampling reduce potential sources of contamination. This requirement seeks to identify opportunities to reduce handling and sample preparation between DNA field collection and laboratory analysis processes, with a specific focus on collection devices.

Challenge: to have a DNA collection device (ie swab, tapelift or other) available that allows the effective collection of biological material and the ability for crime scene personnel in the field to collect the sample in a way that is ready for automated (robot) DNA analysis. This is to minimise the potential for contamination and the need for further handling and sample preparation.

Requirements: The collection device will need to be:

a. Sterile and DNA free (including any accessories within a kit). Ideally be certified DNA Free or accredited under ISO 18385 but this is not essential;
b. Enable the collection of a range of sample types (ie touch DNA and body fluids);
c. sample to be housed in a breathable low bind plastic tube (tapered or skirted), no more than 2ml in size that is compatible with current automated DNA platforms utilised in Australia for use directly on DNA instrumentation without the need for further handling.
d. Ensure the sample, if required, can dry whilst being stored to avoid degradation and prevent mould growth.
e. Post Collection:
    i) temperature stable to allow for transportation and storage, without the need for refrigeration;
    ii) the collection device must easily be “ejected” or separated from its receptacle/holder post DNA collection, not snapped off. Ideally, be “DNA ready” and be stored, transported and submitted directly to the DNA lab without further handling.
    iii) ideally, sample would not need to be subsampled prior to DNA Analysis.

As the primary uses of the collection device is for DNA collection and analysis the collection device will need to:

a. be composed of a material that effectively fixes DNA containing cells during the collection process as well as subsequently readily releases DNA containing cells during the extraction process and does NOT inhibit the DNA amplification process;
b. ensure reproducible results in relation to DNA quantification and amplification;
c. be subject to quality assurance processes and suitable for use under relevant forensic laboratories accreditation requirements ISO/IEC 17025 minimum sterile and DNA Free; and
d. ideally come in kit including the collection device, storage tube and tamper proof transport container in one.

Challenge 3: Digital Forensics Tools

Use Case: In a rapidly evolving digital lifestyle we are surrounded by electronic devices that serve to make life easier with little manual effort, but these devices are also well placed to assist law enforcement in solving criminal investigations. This reliance on technology has the ability to assist in bringing to justice those who compromise the safety and security of our communities during the commission of community crimes such a burglaries, kidnappings and assaults. The abundance of these devices, the pace at which they evolve on the commercial market and ownership habits pose a challenge for analysts in forensic fields who assist in piecing together the series of events that have occurred or analyse evidence to support or refute the circumstances of an incident or event. Encryption of devices adds a further level of complexity in a bid to keep up with technology.

Challenge: This challenge seeks to explore the detection, access, extraction and exploitation of electronic devices with a focus on personal devices and IoT and their assistance to solving community crime. Our reliance on digital and electronic products in our daily lives continues to increase as technologies evolve. Many of these consumer technologies have the ability to collect and store vast amounts of information. The biggest challenge in this area is the development of innovative digital tools that are diverse enough to analyse data from a wide variety of digital sources into a useable format, as opposed to specific software for each electronic device. The growth and utilisation of the internet and technologies like Bluetooth and wifi can now commonly be used to connect electronic devices such as mobile phones to control lights, televisions, fridges, cameras, vacuums, drones and vehicles. There is a need to determine novel ways to utilise the evolution of technology in our lives as a means of solving more community crimes by answering the traditional forensic principles of "who, what, where, when, how and why". Another area of focus is attribution, and creating tools that can assist with identifying those who are on, using or connected to specific devices. An additional challenge is how to sort and manage large data sources in an intuitive way to extrapolate relevant information.

Requirements: Potential areas of research in this area may include:

- Processes and software that can verify data trails and data acquisition to ensure authenticity of data that meet the evidentiary requirements for court purposes.
- Reliable and analytical tools that are intuitive to exploit a broad range of existing and emerging electronic devices and platforms within the region of Australia and will be subject to validation processes.
- IOT capabilities of personal and-home based devices including, but not limited to, fridges, televisions, lights, vehicles.
- Platforms/tools that can assist with encryption related to devices, applications or cloud data.
- Exploring the scope to leverage devices within households and businesses that are specific to Australia.
- Intuitive tools to manage and exploit large data sets.

About NSSTC

The National Security Science and Technology Centre (NSSTC) within Defence Science and Technology Group (DSTG) coordinates whole-of-Government science and technology for national security. It strives to partner widely across the community in order to improve impact, encourage alignment and reduce duplication. To achieve this, NSSTC fosters industry, academic and international partnerships to build a targeted national science and technology capability and leverage state of the art capabilities for Australia.

The NSSTC is responsible for:

- Coordinating whole-of-government national security S&T
- Fostering industry and academic S&T partnerships

- Fostering international research collaboration through partnerships.

There are six National Security Science and Technology Priorities that function within the centre to drive strategic advantage by clearly articulating requirements and challenges, assisting to shape and influence programs of work across the national security agencies and the broader science and technology ecosystem.

The six NSST Priorities are:

- Technology Foresight;
- Intelligence;
- Preparedness, Protection, Prevention and Incident Response;
- Investigative Support and Forensic Science;
- Border Security and Identity Management; and
- Cyber Security.

Expected Delivery

The expected outcome for all funded proposals will be the demonstration of a prototype solution in a simulated use case environment. The expected technology readiness level (TRL) is 5-7 and will represent sufficient functionality for national security specialists to make a preliminary assessment of functionality and performance via a demonstration of capability in a representative environment.

Existing technologies that might be realigned to meet the needs of this call are also open for investigation. In this case we understand that current equipment TRL levels may be suppressed when redefining equipment and demonstrating in a new area.

Closing Date

Proposals are to be submitted via the online form by midnight (AEDT) **Monday 31st January 2022**

Selection Criteria

1. **Alignment with S&T challenge requirements**

   The extent to which the outputs generated will address the challenge requirements and provide a technological advantage.

2. **Expected enhancement to national security capability**

   The extent to which the proposed innovation has the potential to improve or contribute to Australia's National Security capability and capacity. This includes benefits to industry and the commercial potential of the expected outputs, and any spill-over benefits.

3. **Industry involvement and co-investment**

   The extent to which the proposal is being conducted by or engages with an Australian business, as well as any in-kind or cash contributions being made to the project as a co-investment.

4. **Feasibility of the approach and capability delivery**

   The current technology readiness level of the proposed innovation, and the relevance and credibility of any claims made by the respondent relating to the feasibility of the proposed innovation (including about the skill, knowledge and track record of the team to deliver the proposed project).

Eligibility

Proposals are sought primarily from Australian industry as well as research organisations, Publicly Funded Research Agencies (excluding DSTG) and universities. Proposals can be from a single organisation or from collaborative partnerships. Proposals which are from an industry partner or in collaboration with an industry partner will be viewed favourably and weighted accordingly in the selection criteria.

Please see the Conditions of Funding for Citizenship and Security requirements concerning nominated personnel on the proposal.

Conditions of Funding

- Personnel involved in the project must be resident in Australia and either
  - an Australian citizen; or
  - an Australian Permanent Resident.

  Proof of citizenship or residency status must be provided if requested.
- Proposals should be submitted ideally from Australian incorporated businesses or from research organisations that are collaborating with an industry partner. Whilst proposals from academia alone are eligible, those proposals including industry partners will be viewed favourably and weighted accordingly in the selection criteria.
- The project proposals will be subject to a sensitivity assessment to assess if there are national security sensitivities or classified materials being generated or exchanged. Where required, the Project may be required to apply security controls and personnel must agree to be subject to a Security and/or Police check if requested. Personnel on the project may also be restricted to Australian Citizens only. If security clearance are required, personnel must receive a favourable assessment before being allowed to commence work on the project.
- A licence must be granted to the Commonwealth to be able to use intellectual property developed as part of the project. This licence is included in the project agreement and is for Commonwealth purposes.

Intellectual Property

Ownership of intellectual property developed using the funds will be retained by the successful applicants. All successful applicants will be required to grant a licence to the Commonwealth to use project intellectual property for Commonwealth purposes, as part of the project agreement.

Contracting Information

Industry or PFRA Led Responses: All agreements between the Commonwealth and an industry or PFRA applicant shall be entered into under the same conditions as the Next Generation Technologies Fund Research Contract. A sample NGTF Research Contract can be downloaded here.

University Led Responses: All agreements between the Commonwealth and a university applicant shall be entered into under the existing Defence Science Partnering (DSP) Deed as a Standard Research Project. Costings for the work should be calculated accordingly (as per the DSP Costing Model as defined in Schedule 3 of the DSP). A sample DSP Research Project Agreement can be downloaded here.

There is no scope for negotiation on individual terms outside of the project schedules. Please ensure your organisation is comfortable with key obligations such as IP, security and compliance with Commonwealth legislation.

Contracting is expected to be completed by, and projects commence in, March 2022.

Project Milestones and Deliverables

Each project will be required to provide 6-monthly progress reports, a final technical report, demonstrate the prototype in an appropriate environment and provide the prototype and training in its use so that it can be fully assessed.

All projects are to provide a detailed confirmation of proof-of-concept and a prototype plan within 8 weeks of contract execution.

Applicants are asked to propose progress milestones and (if appropriate) additional deliverables that will allow progress to be adequately monitored.

The prototype deliverable will be at Technical Readiness Levels (TRL) 5-7 or above.

Fixed Deliverables	**Weeks from contract execution**	**Expected Date** (24 month projects)
Confirmation of proof of concept / prototype plan	8	April 2022
Progress Report 1	26	September 2022
Progress Report 2	52	March 2023
Progress Report 3 (if applicable)	78	September 2023
Prototype Delivery & Training in Use	104	March 2024
Final Report	104	March 2024

Projects of 18 months duration will be expected to submit their final report and deliver the prototype and training in September 2023.

NSSTC reserves the right to terminate the contract at any time if sufficient milestones and deliverables are not met throughout the duration of the project.

Completing the Proposal

The proposal is to be submitted via the online form.

Project Leader – The Project Leader will have overall responsibility for the direction of the project. For collaborative projects, the employer of the Project Leader will usually be the lead contracting organisation.

The Proposal – the proposal is to be uploaded as a pdf of no more than **3 x A4 pages** excluding references and budget. Your proposal should include

- a brief statement of the research problem you are addressing and how solving this will contribute to meeting the capability requirements of the challenge;
- a description of the prototype you are aiming to achieve;
- the approach you will take to the problem and why you believe this will work;
- how you will know you have succeeded in your approach, and how will you know you are making progress along the way (ie milestones);

- a brief statement on the alignment of this project with the R&D priorities and strategic goals of your organisation. Defence and National Security are interested in developing long-term relationships and building national capability; and
- If applicable, a brief statement describing the level of industry engagement or the collaborative relationship, especially for university-industry partnerships. This is not required for single industry-only proposals.

Budget, Personnel, Milestones and Deliverables – Use the SAT Challenges spreadsheet available on the website.

Requested budget items are to be entered on the first page of the spreadsheet. Please add more rows to sections if needed.

Please ensure the correct organisation type is selected in cell B5 of the sheet before entering cost items, as this is used to determine if the overhead multiplier is used.

All expenditure items are to be entered as exclusive of GST.

The budget must include all nominated personnel who will work on the project, both those who will receive their salary from the project and any who will be in-kind contributors. The citizenship details must be provided for any named personnel. Select their status from the drop-down menu in column C. If 'Australian Citizen' is selected, the country of citizenship will automatically be shown as 'Australia'. Other countries of citizenship must be manually entered. For proposed positions that will be recruited, include the organisation where you are planning to employ them (if you are collaborating) and leave the citizenship cells empty.

Industry / PFRA led responses – enter your usual charge-out rate for each staff member or item, inclusive of salaries, on-costs, and organisational overheads. No overhead recovery multiplier will be applied.

University led responses - enter the direct employment costs for each staff member – that is the base salary plus all on-costs applicable to your organisation (ie superannuation, payroll tax, workers compensation insurance etc). Do not add the 1.4 overhead recovery multiplier here. This will be applied to the project total automatically at the end.

Co-investment in the project will be viewed favourably and weighted accordingly in the selection criteria. Co-investment demonstrates your organisation's commitment to ongoing efforts related to addressing national security requirements. Co-investment in the project is not mandatory. If there are more than one organisation involved in the project, the name of the organisation making any co-contribution is to be included in column H (Notes).

A very brief justification for requested funding items is to be included in column H.

Proposed project milestones and any additional deliverables are to be entered on the second page of the spreadsheet. Milestones must be sufficient to gauge how well the project is progressing over time. Please note, projects which do not meet agreed milestones may be terminated.

For projects of less than 24 months, please delete deliverable 4 (progress report 3) and adjust any later deliverable dates as necessary.

Research Publications and Patents - You may also provide an additional **2 x A4 pages** of relevant research publications and patents by team members. This is not compulsory.

Information Sessions

The NSSTC will provide an online briefing about each challenge to interested parties. This will provide an opportunity for clarifications and questions to be raised.

Challenge Topic	Details
Challenge 1: Safe Vehicle Interdiction	Date: Thursday 16th December Time: 2-3pm AEDT
Challenge 2: Enhanced Crime Scene DNA Collection	Date: Thursday 16th December Time: 3:30-4:30pm AEDT
Challenge 3: Digital Forensics	Date: Monday 13th December Time: 12:30-1:30 AEDT

Please register your interest to attend the session(s) using the link provided by the facilitation network in your state. Any further questions after these briefings which aren't answered here or in the linked associated documents will need to be provided in writing by email to the contact address detailed below.

Applicant Location	Facilitation Network	Contact email
Victoria	Defence Science Institute (DSI)	DSI_NSSTC21@defencescienceinstitute.com
NSW	Defence Innovation Network (DIN)	info@defenceinnovationnetwork.com
South Australia	Defence Innovation Partnership (DIP)	enquiries@defenceinnovationpartnership.com
Western Australia	Defence Science Centre (DSC)	DSC@jtsi.wa.gov.au
Queensland	Queensland Defence Science Alliance (QDSA)	info@queenslanddefencesciencealliance.com.au
Tasmania	Defence Science Institute (DSI)	DSI_NSSTC21@defencescienceinstitute.com
ACT	Defence Innovation Network (DIN)	info@defenceinnovationnetwork.com
Northern Territory	Defence Innovation Partnership (DIP)	enquiries@defenceinnovationpartnership.com