



Network Plus for Analytical Behavioural
Science in Security and Defence

Research for understanding and mitigating risks to security and defence

Second Topic Announcement

Call Specification

Table of Contents

1	Introduction.....	3
1.1	Background	3
2	Invitation	3
2.1	Types of proposals and duration	3
2.2	Topic focus	4
2.2.1	Organisational Resilience and Staff Wellbeing	4
2.2.1.1	Staff Wellbeing and Resilience	4
2.2.1.2	Wellbeing Evaluation Framework: Value for Money.....	5
2.2.2	Trust and Reputation in Anonymous Online Spaces	6
2.2.3	Socio-Cultural beliefs and Decision-Making	7
2.2.4	Hackers & AI.....	8
2.2.4.1	Bottlenecks in the attack pathway	9
2.2.4.2	Hacker ‘intuition’ as a constraint on AI adoption.....	9
2.2.5	Covert and Overt Surveillance in Law Enforcement	9
3	Funding.....	10
4	Application process	11
4.1	Response format	11
4.2	Eligibility.....	12
4.3	Submission	12
4.4	Assessment process.....	12
4.5	Assessment criteria.....	13
5	Grant Conditions.....	14
5.1	Engagement with NABS+	14
5.2	Communication and data-sharing.....	15
5.3	Reporting	15
5.4	Intellectual Property.....	15
5.5	Ethics	16
5.6	Security issues.....	16
6	Commissioning Timetable.....	16
7	Further information	17
8	Appendices	18
8.1	Appendix A	18
8.2	Appendix B	22

1 Introduction

The UKRI funded NetworkPlus for Analytical Behavioural Science in Security and Defence (NABS⁺), in part-collaboration with L-PACE (Lancaster Policing Academic Centre of Excellence) and CRANE (Cyber Security Research and Networking Environment) is commissioning synthetic and original research activity to address current challenges facing the UK. This Call Specification outlines our ambitions, the type of funding available, and the process by which eligible bodies may apply.

1.1 Background

NABS⁺ seeks to develop the next generation of analytical behavioural science and scientist for national security and defence. Its community of academic, government, and industry experts hold in common an interest in using new forms of data and analytics to improve public safety in areas of risk, inference, influence, and futures (more information on NABS⁺ is available at: <https://crestresearch.ac.uk/nabs/>).

NABS⁺ supports its members through workshops and conferences, funding to deliver small projects, training, and knowledge exchange. This Commissioning Call is an opportunity to help NABS⁺ deliver relevant small projects. Individual researchers and research teams in academic institutions, research organisations, SMEs, and industry are eligible to receive commissioning funds (see Section 4.2 for full eligibility details). Successful applicants will benefit from the central resources NABS⁺ can provide to help with translating and communicating evidence for impact, and opportunities for sustained interaction with the user community.

2 Invitation

2.1 Types of proposals and duration

Applicants should propose a programme of work that addresses **one** of the topics identified in Section 2.2. It is anticipated that applications which simultaneously address multiple topics will be too broad in scope to be effective. Applicants may submit more than one proposal. **A project may last no more than 6 months, unless you are submitting a proposal to the surveillance requirement (Section 2.2.5), where projects can last up to 12 months.**

A project may include costs for workshops or other innovative dissemination activities that have clear objectives and offer more than what might reasonably occur at existing conferences or meetings. Where possible, the outcomes of these events should be of value to, and have impact on, an audience broader than the workshop attendees (e.g., by publishing a workshop report).

2.2 Topic focus

Applicants are invited to submit proposals for projects on the following topics. In some cases, the focus of the call is the synthesis of existing research. In other cases, the focus is on original research. The focus is stated in each topic description. Proposals that offer a focus not requested (e.g., original research when a synthetic review is requested) will be considered out of scope. **In all cases a successful proposal should consider issues of ethics and application within the topic area.** We welcome proposals that emphasise and/or seek innovate approaches to promote ethical and responsible research practices.

2.2.1 Organisational Resilience and Staff Wellbeing

How can an organisation operating in high-threat, high-uncertainty environments design and run its crisis functions and sustain the wellbeing and resilience of its people? NABS+ is interested in funding work to help increase our understanding in these areas. We are interested in synthesised evidence, behavioural data and analytics that can strengthen understanding (i.e., the measurement of what people and teams do), prediction and evaluation, and the methodological and ethical limits of taking such approaches.

2.2.1.1 Staff Wellbeing and Resilience

Working in difficult environments, including crisis situations, places demand on people's wellbeing. Many existing wellbeing approaches tend to focus on the individual and what steps can be taken to increase their resilience. NABS+ is interested in understanding the systemic approaches (e.g., organisational culture, team dynamics, structural processes, and organisational design) to wellbeing and resilience in high-stress or crisis-adjacent environments.

We will consider proposals that include one or more of the following – as they relate to high-stress/crisis adjacent environments: (i) synthesis of existing research on systemic wellbeing/resilience interventions; (ii) case studies of organisations that have adopted systemic approaches to wellbeing/resilience; (iii) original research.

A successful proposal is likely to:

- Empirically show (e.g., through meta-analyses) which systemic interventions have demonstrated impact on wellbeing and resilience in high-stress or crisis-adjacent environments.
- Empirically show organisations that have successfully shifted from an individual to a systemic model, or combined elements of both, and identify key lessons on implementation and measures of success.
- Identify which system-level behavioural and organisational indicators (e.g., aggregate patterns in attrition, absence, and uptake of support) can be used to monitor wellbeing and resilience at the systemic rather than individual level, and set out the ethical, privacy and validity boundaries of doing so, recognising that monitoring can itself erode the trust and wellbeing it seeks to protect.
- Highlight barriers to help-seeking: what stops people from reaching out for support when they need it?

2.2.1.2 Wellbeing Evaluation Framework: Value for Money

There is a requirement for a reusable, internally applicable tool to assess wellbeing interventions and demonstrate value for money to internal stakeholders, not a one-off analysis. NABS+ wish to commission research to develop a structured framework that can be applied internally to assess and economically justify wellbeing interventions.

We will consider proposals that draw on a credible evidence base, are grounded in the realities of high-stress and security-sensitive operating environments, and **result in a practical tool** an organisation can apply itself rather than a piece of analysis that must be repeated by researchers each time.

A successful proposal is likely to do the following:

- Produce a structured evaluation framework with associated metrics that can be used across different problem types and contexts (i.e., insider threat scenarios and staff attrition risk) to calculate the value-for-money of different interventions.
- Make a clear, evidence based, distinction between preventative approaches (investment before problems arise, building resilience and culture) and interventionist approaches (responding once problems have emerged).
- Show how the relative value of preventative versus interventionist approaches should be assessed.
- Identify, and empirically justify, metrics that best support economic justification for wellbeing interventions (e.g., reduced presenteeism, lower attrition costs, avoided crisis costs, other).
- Specify the behavioural and workforce data sources the framework would draw on, and assess their availability, quality and validity for calculating value-for-money in practice, including, for insider-threat contexts, the behavioural indicators the framework would rely on and the ethical limits of their use.

2.2.2 Trust and Reputation in Anonymous Online Spaces

Digital crime affects all corners of society from single individuals to large companies to critical infrastructure. In many cases, these crimes are underpinned by a network of threat actors who operate from across the globe and target victims with similar reach. Actors in cybercriminal communities stand to gain from the prestige and reputation-building earned for their efforts, such that they may gain access to invite-only forums, experience greater influence in a cybercriminal community, and/or benefit from increased monetary gains. However, malicious cybercriminal communities rely on anonymity and trust between members to be successful. Research examining the development and maintenance of interpersonal trust and reputation emphasise the importance of visual cues, openness, and honesty—cues that are moot in cybercriminal communities that operate on anonymity. This raises the important question of how individuals in anonymous cybercriminal communities form social connections and develop trust and reputation. NABS+ is looking to commission research that draws on behavioural analytics to offer an evidence-informed insight into this area.

We will consider proposals that include original research.

A successful proposal may do one or more of the following **in the context of an anonymous online community**:

- Identify reliable ways that people build and maintain reputation and the conditions under which these are most effective.
- Empirically demonstrate if the same factors are implicated in reputation-building as in reputation-degradation, and whether reputation can be recovered.
- Offer an evidence-informed understanding of the factors (behavioural, social, cultural) that supports a person's initial entry into a group.
- Identify effective, long-term, ways to damage a person's reputation, and/or trust online.
- Identify how the context of an anonymous online community influences the process of reputation-building and reputation-degradation (e.g. does the type of illicit activity or nationality of community members change how members build reputation?).
- Identify whether and how reputation and trust may develop differently between cultures.
- Identify whether attribution of trust or reputation adapts following a technical change to platform. If so, how?

2.2.3 Socio-Cultural beliefs and Decision-Making

Cross-cultural research has highlighted the importance of understanding decision-making in the social and cultural context that a person finds themselves within, and the personal belief and value systems they hold. These belief systems may be underpinned or driven by the religious, ethical or philosophical systems common to a society or culture. Beliefs and values that drive behaviour are manifold and may be stratified into, *inter alia*, national, strategic, organisational, mundane, sacred, and moral. They may intersect and/or influence decision-making in different contexts.

NABS+ is interested in commissioning original research that draws on behavioural analytics to offer a nuanced understanding of the role of belief systems on decision-making and the conditions under which a set of beliefs may be most pertinent and most influential on decision-making. This can include both the behavioural outcome of the decision (e.g., online behaviour, engagement in risky or illicit behaviours, help seeking) and the associated cognitive process by which the course of action is selected (e.g., selection and prioritisation of information).

We are **not** looking to fund research that considers a single belief or value system (e.g. sacred values), but rather are interested in a consideration of multiple socio-, cultural- beliefs. Research that takes a cross-cultural approach or considers non-Western cultures and belief systems will be favoured.

We will consider proposals that include original research.

A successful proposal may do one or more of the following:

- Empirically show whether (and what) belief systems can be identified through an individual's offline and/or online behaviour.
- Identify how belief systems influence the cognitive process by which individuals select a course of action.
- Identify the relative influence of different beliefs systems on decision-making, and the conditions under which different belief systems are most influential.
- Identify which beliefs – as measured through online behaviours – have the strongest impact on behaviours.

2.2.4 Hackers & AI



AI technologies are being developed and used by both attackers and defenders. Given the pace of advancement, there is a risk that these technologies benefit attackers before defenders unless potential risks are anticipated. An important element of effective defence is understanding the likely trajectory of the technology on the attacker side, so that responses can be prepared in advance.

The challenge is sociotechnical rather than purely technical. AI does not currently present a step-change in risk across the cyber attack chain, but how offensive capability develops will depend on attacker behaviour and incentives as much as on the underlying technology. Attackers are not uniformly capable: they encounter friction, dead ends, and tasks that resist automation. Where that friction sits, and how tolerable it is, plausibly shapes where AI gets adopted first and where it stalls.

NABS+, in collaboration with CRANE, are interested in funding short, focused projects that examine how attacker behaviour may influence the development, testing and adoption of AI by threat actors. Projects are expected to produce transferable insight for defenders within six months, rather than to complete a definitive study of the field.

Applicants should address one of the two topics below, or propose a single integrated project spanning both where the connection is clearly argued. Proposals addressing both topics in parallel without integration will not be competitive at this scale.

We will consider proposals that include one or more of the following: (i) a synthesis of research, (ii) secondary analysis of existing incident, threat intelligence or competition data, or (iii) original research.

We are looking for tightly bounded designs that make efficient use of existing access and evidence. Suitable approaches include structured expert elicitation with red teamers, penetration testers, CTF competitors and incident responders. Applicants should state clearly what access, data and ethics is already in place at the point of application.

2.2.4.1: Bottlenecks in the attack pathway

Where do attackers encounter genuine friction, and what does that imply for AI adoption? Proposals should address:

- The specific pain points attackers face at different stages of an attack (for example, reconnaissance, initial access, exploitation, lateral movement, evasion, monetisation), and how these differ by actor type and sophistication.
- The cognitive, organisational and technical factors that produce these bottlenecks — including which are artefacts of tooling and which reflect harder limits on judgement, context or trust.
- What relieving a given bottleneck would mean for attack economics, and which bottlenecks AI is plausibly positioned to relieve in the near term versus those it is not.

2.2.4.2: Hacker 'intuition' as a constraint on AI adoption

How far does offensive success rest on tacit expert judgement, and is that judgement a barrier to automation? Proposals should address:

- The relative contribution of adversary 'intuition' and available tooling to attack success.
- How experienced adversaries acquire and apply intuition in decision-making, and how they recognise it in others.
- The heuristics, biases and situational cues underpinning "hacker intuition", including where these help attackers and where they mislead them.
- A characterisation or model of this expertise, together with a specified design for how it could be captured, evaluated, or applied in a security testing context. Projects should deliver the framework and a credible demonstrator design or pilot (**building and validating a working tool is out of scope at this duration**).

2.2.5 Covert and Overt Surveillance in Law Enforcement

Surveillance has long been a cornerstone of effective law enforcement. Advances in technology have transformed the surveillance landscape for both overt and covert capabilities as well as the challenges of counter-surveillance.

While directed and intrusive surveillance has been subject to governance through the Regulatory of Investigatory Powers Act (RIPA, 2000), surveillance by law enforcement more generally faces a range of technological, psychological, social and behavioural challenges.

NABS+, in collaboration with L-Pace, are interested in funding a 12-month project that seeks to re-examine questions that have long been associated with law enforcement surveillance – but which may have taken on different forms in the light of modern technological developments. Questions of interest include: How do officers determine the veracity of surveillance data that comes from different modalities (e.g., visual audio, sensor) and different spaces (e.g., public/private); all of which may be vulnerable to being 'faked' or manipulated? How might extensive surveillance data impact the complexity of decision-making for officers? How do contextual factors, such as time pressures, interact with officer handling of surveillance data? How we can better support staff to manage the social and behavioural challenges of covert surveillance in the digital age?

We will consider proposals that include original research.

A successful proposal is likely to do one or more of the following:

- Empirically identify how people verify if surveillance material is genuine and trustworthy.
- Offer an evidence informed understanding of how people manage and make decisions when faced with multiple streams of information, of which some may be inauthentic.
- Identify support mechanisms (social and/or technical) that aid human decision-makers when dealing with surveillance data overload in uncertain environments.
- Identify support mechanisms (social and/or technical) that support the welfare of staff engaged in covert surveillance in the digital age.
- Couch their work in law enforcement or in a context with close parallels.

3 Funding

It is intended that the total amount available for this Call will be up to £610K at 100% full Economic Cost (fEC), of which 80% fEC (i.e., up to £400K) will be made available to successful applicants.

The upper amount that each applicant may request for Topics 2.2.1 to 2.2.4 is £60,000 @100% fEC (£48,000 @80% fEC).

The upper amount that may be requested for Topic 2.2.5 (Surveillance) is £100,000 @100% fEC (£80,000 @80% fEC).

In practical terms this means that UK HEI researchers should cost their projects using the same process as they would cost a UKRI grant. All other applicants must recognise that an application to NABS⁺'s commissioning programme requires a commitment to provide the remaining 20% of full Economic Cost from their own resources. That is, NABS⁺ will pay 80% of the total costs outlined within the proposal. All costs should be inclusive of VAT and/or any other applicable tax. A guide to fEC and the ESRC's position on its payment is available at: [Terms and conditions for research grants – UKRI](#).

The duration of work proposed for topics 2.2.1 to 2.2.4 should not last more than 6 months and may commence from December 2026 and finish no later than November 2027.

The duration of work proposed for topic 2.2.5 (surveillance) should not last more than 12 months and must finish by December 2027.

No cost extensions will not be possible on any of our funded projects.

NABS⁺ will not reimburse costs associated with the development or submission of a proposal.

All projects will be assessed on an individual basis against the Assessment Criteria in Section 4.5.

4 Application process

4.1 Response format

Applicants must ensure that their proposal conforms to the format specified in Appendix A of this Call. Proposals must be costed and approved by the applicants' organisation authority before submission. The costings submitted should represent the 100% full Economic Cost (fEC) of completing the project, but applicants should recognise that they will receive only 80% fEC in accordance with normal UKRI practices (see Section 3). The costings submitted should be sufficiently detailed to enable the assessors to make informed judgements about the project's value for money.

4.2 Eligibility

The Call is open to Higher Education Institutions, research organisations, charities, commercial companies, and individuals from the UK and overseas who can demonstrate a capability to deliver a high-quality piece of research. Interested partners without such experience should consider partnering with established research institutes. We strongly encourage applications from researchers in all disciplines of the economic and social sciences, conceived broadly. We also encourage proposals that are interdisciplinary and that involve collaborations between stakeholders and researchers. Researchers who have not traditionally worked in the security or defence domain but believe their expertise may provide insights or new applications to the area, are particularly encouraged to apply.

4.3 Submission

Applicants must submit an electronic copy of their proposal. An electronic copy must be emailed to nabscommissioning@lancaster.ac.uk by **17:00 on 20th October 2026**. The electronic submission must be in a single document of PDF format.

Proposals that do not meet the format requirements (see Appendix A), or are submitted after the deadline, will not be considered. This includes proposals that are over length or submitted as multiple documents.

NABS+ will treat all proposals as competitive information and will disclose their contents only for the purpose of the commissioning assessment process. Copies of unsuccessful proposals will be destroyed at the conclusion of the evaluation process. Full details of submission requirements can be found in Appendix A.

4.4 Assessment process

The selection of one or more proposals for award of the commissioning funds will be based on a transparent, competitive evaluation process. Once accepted, full proposals will be sent to: (1) at least three expert peer reviewers who will be asked to assess the proposal against the Assessment Criteria (see Section 4.5); and (2) an expert user reviewer who will be asked to assess the proposal against the Pathways to Impact criterion of the Assessment Criteria.

These assessments will inform the evaluation of proposals by a specially convened Commissioning Panel that comprises the NABS+ Director, representatives from L-Pace and CRANE, external representatives from the

NABS⁺ community, and representative(s) from UK defence and national security to comment on 'impact' and fit to requirements (we may increase the number of external representatives should the number of submissions require it).

As part of a submission, applicants are invited to nominate up to two academic peer reviewers, however, only one nominated academic reviewer will be approached. Applicants must ensure that nominated reviewers have no known conflicts of interest. **Applicants must ensure that they seek the reviewer's permission before nominating them.** Applications that do not nominate reviewers will not be disadvantaged.

We reserve the right to reject proposals that are deemed to fall outside the remit and scope of this call, without reference to peer review. Applicants are advised to contact NABS⁺ if they are unsure whether their proposal will be suitable for the call (see Section 7 for further information).

4.5 Assessment criteria

Applications will be assessed by reviewers and the commissioning panel on the following criteria:

Quality of proposal

- Research excellence and contribution to existing knowledge
- Identifies questions central to the remit of the topic and addresses these directly
- Clear work plan with realistic, testable milestones and clear deliverables
- Addresses risks to, and management of, the project over its lifespan
- Commits to research transparency and integrity, such as engagement with Open Science practices; and articulates how they will engage in responsible research.

Pathways to Impact

- Likely importance and timeliness of research to potential users
- Effectiveness of plans to involve potential stakeholders and users, as well as other NABS⁺ researchers and NABS⁺'s communication mechanisms
- Evidence of well thought-through and realistic dissemination plans to maximise academic/societal/economic impact.

Track record of applicants

- A record of research and research application in the relevant field. This may be a field outside of security or defence research (i.e., this call is not only open to researchers in security studies)
- A record of successful project completion.

Value for money

- Reasonable and fully justified costs for the specified project.

5 Grant Conditions

Applicants who are successful will be required to meet the conditions outlined in the Commissioning Subaward. To facilitate contracting, this contract will be available shortly at: <https://crestresearch.ac.uk/nabs/commissioning/>

Applicants should ensure that they and their organisation are able to meet the conditions of this agreement prior to applying for funding. For transparency, we outline some of the conditions in this Section.

5.1 Engagement with NABS⁺

One of the unique elements of NABS⁺ funding is that we work actively with researchers to support the 'translation to impact' element of their proposal. All commissioned projects will have a designated NABS⁺ point of contact and support from our core team of communication, events, and programme delivery specialists. They will also be provided with a nominated Research to Practice Fellow who will offer stakeholder experience to advise the applicant on how best to deliver the research. This occurs without impinging on the applicant's independence. NABS⁺ actively encourages inter-project activity with other NABS⁺ researchers and support will be provided to enable this where appropriate.

There is an extensive network of stakeholders associated with the topics proposed in this Call. Stakeholders include UK and overseas government departments, police, businesses and organisations involved with the critical national infrastructure, not-for-profit organisations, and think-tanks. Applicants will be encouraged and should be willing to understand and engage with our stakeholder community.

5.2 Communication and data-sharing

All deliverables from commissioned projects will be expected to be unclassified, in the public domain, and published and disseminated through normal academic and other publication channels. In addition, applicants are encouraged to present their work at conferences, workshops, networks, and other dissemination events, and costs associated with doing so may be budgeted in the proposal.

As per normal ESRC practices, all data collected as part of a commissioned project must be made available at the UK Data Archive (unless a case for exception is made). A record of available data (but not the data themselves) will also be kept by NABS⁺. More details on the UK Data Archive are available at: <http://www.data-archive.ac.uk>.

All academic publications that are produced by the commissioned projects must comply with the ESRC's policy on Open Access (see [UKRI open access policy – UKRI](#)).

5.3 Reporting

Applicants must articulate a set of milestones and specific, measurable deliverables as part of their proposal including an indication of where stakeholder input will be critical to the success of the project. In addition to these deliverables, successful projects will be required to complete a six weekly update report. This report, which takes the form of completing a brief template, is to allow for the early identification of problems so that we can work constructively and quickly to find solutions. A final invoice must be submitted to NABS⁺ within 3 months of the end of contract.

5.4 Intellectual Property

All Commissioned projects will be subject to ESRC's standard terms and conditions in relation to Intellectual Property. These state that the intellectual property (IP) generated through the grant rests with the research organisation that holds the grant. However, wherever reasonable, researchers should expect to share the IP generated with NABS⁺ (L-Pace and CRANE, where applicable) members and other commissioned projects, for wider public benefit and for the purposes of achieving the aims and objectives of NABS⁺. There will be no payments for this use of IP. Our funding organisation and members of UK defence and national security will have the right to copy and use all outputs for any government purposes.

5.5 Ethics

Applicants must ensure that the proposed research will be carried out to a high ethical standard. They must clearly state how any potential ethical issues have been considered and addressed, and they must ensure that all necessary approvals are in place, and that all risks are minimised, before the project commences. All applicants must comply with the ESRC Framework for Research Ethics ([Framework for research ethics – UKRI](#)).

In addition, the applicants' proposed research will be reviewed by the NABS+ Ethics Review Task Force (ERTF). The remit of ERTF is to consider issues particular to defence or security research that may require expertise not available on institutional ethics boards. These issues relate, *inter alia*, to: (1) the potential misuse of the research; (2) the risks and benefits of public sharing, especially to national security; (3) the best way to promote public consumption and ensure transparency; and, (4) the wellbeing and security of personnel. ERTF will offer recommendations to the applicant in a constructive process. An application's proposed research must be approved by ERTF before it is conducted.

5.6 Security issues

Applicants should demonstrate an understanding of any potential personal, cyber- and physical security risks that may stem from their proposed work. This includes paying due regard to overseas travel advice provided by the Foreign and Commonwealth Office. Applicants should outline a risk mitigation strategy in their 'Case for Support', outlining both why the risk is necessary and what steps will be undertaken to mitigate its potential. Further guidance on issues relating to security will be provided by NABS+ to successful applicants.

6 Commissioning Timetable

13 October 2026; 17:00 – Deadline for questions and queries

20 October 2026; 17:00 – Deadline for submitting full proposals

w/c 14 December 2026 – Commissioning panel meeting

December 2026 – Successful applicants informed and award commencement

7 Further information

A list of questions and answers is available at:

<https://crestresearch.ac.uk/nabs/commissioning/faqs/>

If you have questions not already answered, or require further information, please email Susanna Yates (NABS⁺ Project Manager),

nabscommissioning@lancaster.ac.uk

8 Appendices

8.1 Appendix A

All proposals under this Call must be completed using the requirements outlined in this Appendix. NABS⁺ reserves the right to reject any submission that does not conform to these requirements.

All sections outlined below are mandatory, and applications must not exceed the maximum length of each section. Applicants should include the section with the entry 'Null' if they do not believe it is relevant to their submission. **Applications should use Arial font at a minimum size of 11pt. Margins should not be narrower than 2cm.** The use of diagrams, tables, and other graphics that aid comprehension is encouraged.

The following sections must be included in the proposal which should consist of **no more than 12 pages** (excluding additional references and CVs, see below):

Cover Page (2 page maximum)

You must complete the provided cover page which can be found in Appendix B or available as a downloadable as a word doc at:

<https://crestresearch.ac.uk/nabs/commissioning>

Applicants must adhere to the specified word count.

Summary (1 page maximum)

- Describe the proposed research in simple terms in a way that could be publicised to a general audience

Pathways to Impact (1 page maximum)

- **Academic impact.** Describe the anticipated and/or potential contribution of the proposed work to academic knowledge and how the proposed work will ensure that this will be achieved. Such contributions may include significant advances in understanding, methods, theory and application, both across and within disciplines.
- **Stakeholder impact.** Describe the anticipated and/or potential contribution of the proposed work to enhance stakeholder understanding of, and their capacity to, mitigate or counter security/defence threats. Describe plans for dissemination, stakeholder involvement and production of any resources that includes how you

anticipate these activities having a positive effect on practice and/or policy.

Stakeholders should be understood broadly to refer to law enforcement, UK Home Office, UK security and intelligence agencies, other government departments, industry, charities and not-for-profit organisations, and, where relevant, the public. It is not anticipated that all proposals will have impact with all stakeholders. Rather, applicants should demonstrate a considered understanding of who is the target audience for their work and what impact it will have.

Case for Support (4 page maximum)

- **Introduction.** Describe the aims and objectives of the study in context, briefly outlining the main work on which the research will draw, with references. Any relevant policy or practical background should be included
- **Research questions.** The detailed research questions to be addressed should be clearly stated
- **Design and method.** Give a full and detailed description of the proposed research methods, or workshop design. Where data collection is involved, the data, materials or information to be collected should be clearly stated, and the procedures for achieving this explained and justified. Where access to people or archives is needed, indicate clearly the records, population or samples to be consulted and the steps that have been taken to ensure this access (bearing in mind that all outputs from commissioned projects must be unclassified). Particular care should be taken to explain any innovation in the methodology or where you intend to develop new methods.

Project Management, Timetable and Outputs (2 page maximum)

- **Work package descriptions.** Identify a breakdown of the work proposed and provide objectives and scope for each work package.
- **Timetable.** Give a clear and structured account (e.g., using a Gantt chart) of the timing of activities that will take place over the period of the grant. Within this timetable identify clear milestones against which the Work Packages will be delivered, and progress may be judged.
- **Deliverables.** Identify the deliverables of the project and justify the choice of medium. Deliverables may include, but are not limited to, academic publications, training materials, briefing notes, reports, technology demonstrators, multimedia presentations, and toolkits. Applicants are encouraged to be innovative in the deliverables they offer, giving particular attention to what will be useful for stakeholders.

As part of delivery, all projects will produce a final report whose structure reflects that of a typical academic publication. Using a NABS⁺ template, the report should include but not be limited to the following sections (1) one-page abstract/executive summary; (2) two-page key-point summary/discussion; (3) introduction/background; (4) methods/approach; (5) results; (6) discussion; (7) Images, figures, graphs and data tables; (8) references; and (9) appendices.

- **Risk mitigation.** NABS⁺ is committed to funding excellent research, which is ground-breaking and innovative, and has the potential for high scientific and/or user impact. Describe the anticipated and/or potential risks to the research including ethical and management issues. Please outline any measures which will be taken to mitigate them.

Summary of Resources Required (1 page maximum)

- **Staff costs.** Identify each contributing member of staff and how many hours per week they will work on the project, the cost of this contribution in GBP (£), and an outline of what they will contribute.
- **Travel and subsistence.** Identify each trip proposed, provide the cost in GBP (£), and provide a short justification for this trip and its costing. This should include trips associated with final deliverable(s).
- **Other costs.** Identify at the per item level other costs that are being requested under the application (e.g., for equipment, licensing, fees), provide the cost amount in GBP (£), and provide a short justification for this item and its costing.
- **Indirect costs.** Identify the indirect costs in GBP (£) associated with completing the proposed project.
- **Total cost.** A summary of total proposal cost in GBP (£).

Capabilities and Relevant Expertise (1 page maximum)

- **Past performance and related work.** Describe a record of performance by the applicant(s) in completing activities (either workshops or research) relevant to the proposed work. Include details of current and complementary work and how this project may connect with this work, as well as how this work will be distinct from any related work. We welcome applications from researchers at all career stages. Early career applicants may include additional costs for the time of a co-investigator's mentoring/support where doing so will help them develop their project leadership experience. Applicants may also describe existing connections with stakeholders that will be leveraged to ensure the proposed work has impact.
- **Synergies and added value.** Describe how this project interrelates with, or adds value to, other ongoing or recently completed research.

Identify how this project will be distinct from past or current work. If this proposal will receive support in kind from other organisations or the host institution(s) of the applicant(s), then this should be outlined in this section.

- **Security and ethics.** Describe the applicants' capability for ensuring the ethical integrity of the proposed activity, and the applicants' capability to manage any security risks that may stem from their proposed work.

Additional

- **Reference list.** Provide a bibliography for the references cited in the proposal. There is no formal page limit for this additional material, though typically no more than 2 pages of references will suffice.
- **Investigators' Curricula Vitae.** Provide a CV (Résumé) for each named investigator and research staff, including consultants. Each CV should be no more than two pages. It should give full name, degrees and postgraduate qualifications, academic and professional posts held, a list of relevant and recent publications, and a record of all relevant research funded by the ESRC and other bodies.

8.2 Appendix B

NABS⁺ Commissioning Call Cover Page

PROPOSAL DETAILS	
Title of proposal	
Topic addressed (as per section 2 of call specification)	
Proposed start date	
Cost (100% FEC of project in GBP including all taxes)	

CONTACT DETAILS	
Contact details for Principal Investigator	
Name	
Address	
Post Code	
Work Email	

CONTACT DETAILS	
If you have chosen to nominate a reviewer, please provide contact details below. Please leave blank if not applicable.	
Proposed reviewer 1 Please provide name, institution and email address	
Proposed reviewer 2 Please provide name, institution and email address	

ADDITIONAL CONTACT DETAILS	
Please provide the for contracting	
Name of contract officer	
Email address	
Name of press officer	
Email address	

SUBAWARD AND SPECIFICATION DETAILS	
Query	Response
As per page 1 point 2, of the subaward, please provide the correct text for the following section: "[INSERT NAME OF PARTY] an [educational body created by Royal Charter/limited company registered in England and Wales under Company Number #####] of [insert address] (the "Contractor")"	
As per section 11, page 10 of the subaward, please provide response to the following section: "The Contractor's representative for the purpose of receiving reports and other notices shall until further notice be:" "[INSERT NAME OF PARTY] of [insert address and email address]"	