CENTRE FOR RESEARCH AND
EVIDENCE ON SECURITY THREATS

RESEARCH FOR UNDERSTANDING, MITIGATING AND COUNTERING SECURITY THREATS

Third Broad 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 Behaviour change 4
2.2.2 Information disclosure in online/virtual environments 5
2.2.3 Assessing the health of a relationship 6
2.2.4 Developing, measuring and maintaining rapport across different contexts 6
2.2.5 Moral injury and belief change 7
2.2.6 Individual differences in the adoption and use of new technology 7
2.2.7 Behavioural analytics 8
2.2.8 Human engagement with Artificial/Augmented Intelligence 8
2.2.9 Misinformation and disinformation 9
2.2.10 Violent Domestic Extremism 9
3 Funding 10
4 Application process 11
4.1 Response format 11
4.2 Eligibility 11
4.3 Submission 11
4.4 Assessment process 12
4.5 Assessment criteria 12
5 Grant Conditions 13
5.1 Engagement with CREST 13
5.2 Communication and data-sharing 14
5.3 Reporting 14
5.4 Intellectual Property 15
5.5 Ethics 15
5.6 Security issues 15
6 Commissioning Timetable 16
7 Further information 16
8 Appendix A 17

1 Introduction

The UK Centre for Research and Evidence on Security Threats wishes to commission a programme of activities that addresses some of the current security threats facing the UK. This Call Specification outlines the programme goals, the type of funding available, and the process by which eligible bodies may apply.

1.1 Background

The Centre for Research and Evidence on Security Threats (CREST) was commissioned by the Economic and Social Research Council on 1 October 2015, with funding from the UK security and intelligence agencies until at least September 2020. The Centre's mission is to deliver a world-leading, interdisciplinary portfolio of independent research that maximises the value of economic and social science research to countering UK and international security threats. More information on the scope and purpose of CREST, and the Centre's ongoing research activities, is available at: https://crestresearch.ac.uk

Following the success of our previous commissioning, CREST is again seeking to identify and fund innovative and forward-looking economic, behavioural and social science research that will contribute to our understanding of contemporary security threats, or enhance the UK's capacity to detect and mitigate such threats. Individual researchers and research teams in academic institutions, research organisations, SMEs, and industry are eligible for commissioning funds (see Section 4.2 for full eligibility details). Successful applicants will become part of CREST's larger research programme, benefiting from resources for 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 Requirements identified in Section 2.2. It is anticipated that applications which simultaneously address multiple requirements will be too broad in scope to be effective. Applicants are invited to propose one of two kinds of activity to address a requirement:

- **Short projects.** Lasting no more than 6 months, short projects address a topic in a targeted way. This may be, for example, the undertaking of a systematic review, a data re-analysis, or the construction and analysis of a case study. Short projects also provide a useful mechanism for researchers to propose proof-of-concept activities, such as an initial experiment or demonstrator, that may provide the evidence-base for a subsequent proposal of a larger programme of work.
- **Long projects.** Lasting no more than 12 months, long projects provide researchers and research teams the opportunity to undertake a concentrated piece of work that provides, in a cumulative way, evidence that clarifies our understanding and contributes to practice. Original research in this regard is understood broadly to include case studies, methodological innovation, and all forms of qualitative and quantitative analysis.

Both short and long projects 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.

Details of successful projects from previous rounds of our commissioning are available on the CREST website.

2.2 Topic focus

Applicants are invited to submit proposals for short or long 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 the second paragraph of each topic description.

2.2.1 Behaviour change

CREST is interested in the evidence base for implementing behaviour change interventions and assessing their impact, both offline and online. We are especially keen to understand the extent to which behavioural change models are applicable to non-Western contexts or cultures. With this in mind, we seek proposals that deliver evidence likely to inform either: (1) the planning and design of effective security-related behaviour change interventions, including frameworks for supporting their design; or, (2) effective measurement of the impact of behaviour change interventions within a security context, which may involve the development of novel methods or methods that allow impact to be

distinguished from 'ambient noise.' The work may be relevant to interventions that seek to reduce engagement in criminal or terrorist activities, or reduce the success of hostile actors' attempts to change behaviour (e.g., to support or join terrorist organisations, or influence populations), or promote effective security behaviour among employees either within the UK or internationally.

We will consider proposals that include one or more of the following: i) a synthesis of research; ii) original research.

A successful proposal is likely to do the following:

- For synthesis, provide a comprehensive, cross-disciplinary review of existing research and draw out insights for security contexts
- Develop a framework or measure that can be used to achieve the topic, and ensure this framework can be used by stakeholders (e.g., by providing a training output)
- Not have Countering Violent Extremism (CVE) and CVE interventions as a primary focus.

2.2.2 Information disclosure in online/virtual environments

CREST is interested in how the 'virtual' environment changes people's interactions in relation to information disclosure about sensitive topics. What factors are associated with increased and decreased information disclosure? How do online differences vary across cultures, age groups and other individual differences? What can be done to increase disclosure? The results may be of value in developing approaches to security vetting interviews, or to encouraging public reporting about potential threats.

We will consider proposals for: (i) a research synthesis or (ii) original research. It should consider the effects of different platforms (e.g., chat, email) and different forms of engagement (e.g., interactive) on disclosure.

A successful proposal is likely to do the following:

- Be cross-disciplinary and draw on work using different methodologies (e.g., experimental, 'netnographic')
- Consider research findings across cultures and communities, and across individual differences (e.g., gender, age, ethnicity, experience)
- Be clear about standards of evidence
- Provide reporting that allows users to interrogate the synthesis' findings to inform a particular scenario.

2.2.3 Assessing the health of a relationship

CREST is interested in how to identify a deteriorating or stagnating relationship, so that remedial action can be taken (e.g., in a one to one relationship with an informant). How can we assess the quality of a relationship between individuals, or between individuals and the groups or organisations to which they belong? What are the behavioural correlates of relational factors such as trust, loyalty, and commitment? How can an assessment take advantage of interactions that occur both offline and online? How can assessments (and subsequent actions) best account for individual differences (e.g., due to cultural background)?

We will consider proposals that include one or more of the following: i) a cross-disciplinary synthesis of research on existing methods; ii) an empirical test of a novel, promising method.

A successful proposal is likely to do the following:

- Examine methods for assessing relationship health/quality, rather than the existence of relationships
- Consider how the method's assessment can be used to direct interventions aimed at improving or maintaining the relationship
- Be creative and novel in approach, using methods that may include passive monitoring of behaviour, direct interaction, or surveys
- Pay attention to cultural and cross-cultural factors.

2.2.4 Developing, measuring and maintaining rapport across different contexts

The development of rapport often occurs across a range of contexts, bringing together very short interactions (e.g., Twitter, Instagram) and longer interactions (e.g., in chatrooms, emails and face-to-face) both offline and online. CREST is interested in how to measure, develop and maintain rapport across multiple online contexts, how this crosses over to rapport offline, and the effect of cultural differences on these processes. How can we measure and monitor genuine 'rapport' in short interactions and longer relationships? How can we recognise when rapport is lost? We are interested in improving guidance and toolkits that help investigators address these issues.

We will consider proposals that include one or more of the following: i) a synthesis of research on existing methods; ii) an empirical test of a promising method.

A successful proposal is likely to do the following:

- Pay attention to cultural and cross-cultural factors

- Develop methods that are novel, effective, and evidence-based
- Explore the topic in one or more of a range of interactive, security-relevant settings (e.g., interviews, checkpoints, online)
- Give consideration to the training and/or implementation of the method proposed.

2.2.5 Moral injury and belief change

CREST is interested in better understanding how individuals of different backgrounds and cultures experience "moral injury". There is a degree of psychological injury that comes with the perception/realisation after the event that the actions ordered or recommended by the leadership of a movement or an organisation are not morally justifiable. What can we learn from cross-disciplinary research on how people think about, and deal with, the realisation that actions carried out for a belief system or organisation were not actually morally justifiable. Does avoiding "moral injury" provide a useful way of understanding resistance to belief change? What is known about the effect of individual differences (e.g. age, gender, ethnicity) on susceptibility and resilience to "moral injury"? What are the early signs of such psychological injury, and how can these be identified?

We will consider proposals that include (i) a comprehensive synthesis of research and theories; and/or (ii) case studies that examine the issues raised above.

A successful proposal is likely to do the following:

- Examine moral injury from a range of perspectives

2.2.6 Individual differences in the adoption and use of new technology

CREST is interested in anticipating the security risks posed by future technological advances through a better understanding of user experience. What factors are relevant to the adoption of new technology by different groups (e.g., generations, cultures, communities)? What influences the attractiveness of intended or non-intended functions in emerging technology for different groups? What factors effect decisions to search, or not search, for such functions? How might criminal or terrorist groups adopt or subvert technology for their own ends? Can this risk be predicted and thus mitigated during the design cycle?

We will consider proposals that include one of the following: i) a cross-disciplinary synthesis of research; ii) original research.

It is likely that successful proposals will:

- provide a framework for understanding adoption across multiple groups
- consider diverse perspectives, beyond the security literature, and potentially drawing on insights from industry
- consider what factors may change this pattern of adoption in the future
- draw out practical, evidence-based insights for security personnel.

2.2.7 Behavioural analytics

CREST is interested in further understanding the opportunities and limitations of using indirect, machine-assisted methods to make inferences about adversary intent and capability. Can we predict what an individual's offline actions might be based on their online behaviour? What does threat look like in data? Can inferences be made – or changes be detected – for group-level traits or variables? What are the benefits of drawing on contextual (e.g., group-level, community-level) information to refine inferences about the individual, and how can this be done efficiently? How best can we measure the impact of data issues (e.g., small sample size, heterogeneity) on these methods, and can these be mitigated?

We will consider proposals that include original research.

It is likely that successful proposals will:

- evaluate a particular method or domain in detail to deliver a workable solution to a security problem
- focus on helping investigators prioritise their workload
- not rely on social media data such as that from Facebook or Twitter
- not focus on predicting traditional personality features (e.g., OCEAN, Dark Triad)

2.2.8 Human engagement with Artificial/Augmented Intelligence

CREST is interested in the interaction between human decision maker and artificial/augmented intelligence and machine learning technologies. We seek to better understand how to facilitate the uptake of such technologies among investigators, as well as understand how to prevent over-use and skill-fade among users. What features of machine-learning technologies engender trust and/or mistrust from the user? What can break trust in a technology and, once broken, can it be restored? What are the factors that predict (over-)reliance in the technology's output and can these be mitigated? What factors influence the trade-off between accuracy (e.g., like that observed through the use of neural nets) and explainability (e.g., decision trees) in machine learning models and how does this impact user experience?

We will consider proposals that include one of the following: i) a cross-disciplinary synthesis of research.

It is likely that successful proposals will:

- provide a framework for understanding adoption across multiple groups
- consider diverse perspectives, beyond the security literature, and potentially drawing on insights from industry
- consider what factors may change this pattern of adoption in the future
- draw out practical, evidence-based insights for security personnel.

2.2.9 Misinformation and disinformation

CREST is interested in how and why disinformation and misinformation spread through communities and social networks, and through what means it does so? What are the psychological and social drivers for the spread of dis/mis-information amongst different audiences? How does this vary across culture and demographic and other key audience features? For example, existing technologies are available that make realistic but fake videos of individuals and situations. How "successful" are fake videos in achieving their intent? What influences their success? Are these influences the same across all technologies and message forms?

We will consider proposals that include one of the following: i) a cross-disciplinary synthesis of research; ii) original research.

It is likely that successful proposals will:

- provide a methodology for assessing the impact spread of a message
- considers both message features and the context in which it is presented.

2.2.10 Violent Domestic Extremism

CREST is interested in developing a better understanding of how Violent Domestic Extremism in the English-speaking world and Europe might develop over the next 3 to 5 years. Violent Domestic Extremism in this context is taken to mean "Extreme Right Wing" or "Extreme Left Wing" groups and individuals who promote or carry out acts of violence to influence the government and public in order to advance a political, religious or ideological cause. CREST is particularly interested in approaches that examine the transnational nature of modern Domestic Extremism, the role of political crises in mobilising extremist

actors to violence, and whether reciprocal radicalisation between violent extremist groups is likely to be a factor.

We will consider proposals that include one of the following: i) a cross-disciplinary synthesis of research; ii) original research.

It is likely that successful proposals will:

- provide a framework for understanding and making inferences about the future of the transnational Domestic Extremism
- consider the perspectives of multiple disciplines and multiple methodologies
- consider what critical factors may change the nature of development

3 Funding

It is intended that the total amount available for this Call will be up to £1.12million at 100 per cent full Economic Cost (fEC), of which 80 per cent fEC (i.e., up to £900,000) will be made available to successful applicants. In practical terms this means that UK HEI researchers should cost their projects using the same process as they would cost an UKRI grant. All other applicants must recognise that an application to CREST's commissioning programme requires a commitment to provide the remaining 20% of full Economic Cost from their own resources. That is, CREST 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 of fEC and the ESRC's position on its payment is available at: https://www.ukri.org/files/funding/tcs/fec-questionnaire-pdf/

The duration of work proposed under this Call should not last more than 12 months and should commence between 1 April 2019 and 1 October 2019. CREST 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. However, the following are indicative costs for each activity:

- Short Projects: An indicative cost for this activity is £62,500 at 100% fEC (£50,000 at 80% fEC).

- Long Projects: An indicative cost for this activity is £125,000 at 100% fEC (£100,000 at 80% fEC).

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 RCUK practices (see section 3). The costings submitted should be sufficiently detailed to enable the assessors to make an 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 programme 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 domain, but believe their expertise may provide insights or new applications to the area, are particularly encouraged to apply. Eligible applicants may submit more than one proposal.

4.3 Submission

Applicants must submit both an electronic copy of their proposal. An electronic copy must be emailed to submission@crestresearch.ac.uk by 10:00GMT on 23 January 2019. The electronic submission must be in a single document of PDF format.

Proposals that do not fulfil the format requirements, or are submitted after the deadline, will not be considered. This includes proposals that are over length or submitted as multiple documents.

CREST 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 an independent and 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 panel 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 CREST's director, a second member of CREST's leadership team, and four external representatives. The external representatives are drawn from the UK and international academic and user communities, from a range of relevant disciplines.

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 perceived 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 CREST if they are unsure whether or not 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 equally weighted criteria:

Quality of proposal

- Demonstrated fit to the remit of the call
- Research excellence and contribution to knowledge
- Clear work plan with realistic, testable milestones and clear deliverables
- Grounding in existing knowledge and strong potential addition to the evidence-base

Track record of applicants

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

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 CREST researchers and CREST's communication mechanisms
- Evidence of well thought-through and realistic dissemination plans to maximise academic/societal/economic impact

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 CREST's Commissioning Subaward. To facilitate contracting arrangements, this contract is available at: https://www.crestresearch.ac.uk/commissioning/terms. 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 CREST

All commissioned projects will be provided with a partner from CREST Programme Leads. The role of the Leads is to support the applicant's engagement in CREST to ensure that the benefit of CREST's activities for the applicant is maximised. The assigned Programme Lead will be a world-leading researcher in a cognate area and they will also offer topic expertise and advice to the applicant, without impinging on the applicant's independence.

There is an extensive network of stakeholders associated with the research topics proposed in this Call. Apart from the UK security and intelligence agencies who are the directly-intended users of this work, other stakeholders include UK and overseas government departments, the police, businesses and organisations involved with the critical national infrastructure, not-for-profit organisations, and think tanks. CREST runs a series of activities that enable

researchers to engage with this network. Applicants will be encouraged to take part in such events.

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 the 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 CREST's Centre Manager and made public. More details on the UK Data Archive are available at: http://www.data-archive.ac.uk

All publications that are produced by the commissioned projects must comply with the ESRC's policy on Open Access (see http://www.rcuk.ac.uk/research/openaccess/). As far as possible, CREST will support the Open Access publication of work by applicants who do not have access to an RCUK OA block grant. This will be accomplished outside of the Commissioning process and costs associated with publication charges should not be included within the application.

All publications that are produced by the commissioned projects must also be reviewed by a nominated CREST point of contact for the UK security and intelligence agencies. This is intended to be a light touch and rapid turnaround process and there will be no obligation to make amendments unless draft publications contain information that is in breach of the Official Secrets Act or any confidentiality agreements, or could have a detrimental impact to national security through the disclosure of sensitive, classified and/or personal information.

5.3 Reporting

Applicants must articulate a set of milestones and specific, measurable deliverables as part of their proposal. In addition to these deliverables, successful small and large grant projects will also be required to complete a quarterly 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 CREST 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 CREST members and other commissioned projects, for wider public benefit and for the purposes of achieving the aims and objectives of CREST. There will be no payments for this use of IP. UK security and intelligence agencies 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 (http://www.esrc.ac.uk/about-esrc/information/framework-for-research-ethics/index.aspx).

In addition, the applicants' proposed research will also be reviewed by CREST's Security Research Ethics Committee. The remit of SREC is to consider issues particular to security research that may require the 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. SREC will offer recommendations to the applicant in a constructive process. An applications' proposed research must be approved by SREC 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 CREST's Security Ethics Research Committee to successful applicants.

6 Commissioning Timetable

15 October 2018 – Issue Call Specification
16 January 2019 17:00GMT – Deadline for questions and queries. Note questions will not be answered between 20 December and 2 January inclusive.
23 January 2019 10.00GMT – Deadline for submitting full proposals
13 March 2019 – Commissioning panel meeting
w/c 22 March 2019 – Successful applicants informed
1 April 2019 – Award commencement (or as soon as possible thereafter)

7 Further information

A list of questions and answers provided is available from our website (https://www.crestresearch.ac.uk/commissioning/faqs), if you have any questions not already answered or you require further information please contact:

Nicola Ronan (CREST Centre Manager)
Email: commissioning@crestresearch.ac.uk

8 Appendix A

All proposals under this Call must be completed using the requirements outlined in this Appendix. CREST 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 have at least 2cm margins and use a minimum sans serif font size of 11pt. 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 10 pages (excluding additional references and CVs, see below):

Cover Page (1 page maximum)

- **Project Title.** Provide a succinct title.
- **Principal Investigator.** Provide the Principal Investigator's name and the organization where the Grant will be held
- **Contact details.** Provide a mailing address and email address for the Principal Investigator and Contract Officer (if different)
- **Application Type.** Identify the type of submission within the application as either: Workshop, Short Project, or Long Project
- **Topic addressed.** Identify topic focus using one or more of the numbers indicated in section 2.2 of the Call Specification
- **Proposed start date.** Provide a preferred start date in the format of day/month/year
- **Cost.** Provide the total 100%fEC cost of the project in GBP.
- **Proposed reviewers.** Provide the name(s), mailing address(es), and email address(es) for up to two reviewers, as per Call Specification

Summary (1 page maximum)

- Describe the proposed workshop or research in simple terms in a way that could be publicised to a general audience [up to 4000 characters]

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
- **Risk mitigation.** CREST is committed to funding excellent research which is also adventurous, speculative and innovative, and with the potential for high scientific and/or user impact. Where there are risks associated with such research, please outline any measures which will be taken to mitigate them.

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 threats. Make a case for the importance and the timeliness of the research for potential users. 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 security and intelligence agencies, law enforcement, other government departments, industry, charities and not-for-profit organizations, 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.

Timetable and Deliverables (1 page maximum)

- **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 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. They should also consider how they engage with existing CREST delivery mechanisms, such as CREST Guides and CREST Security Review. Examples of these mechanisms are available at the CREST website.

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.
- **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 applicants 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. 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.