CRANE Phase One Pilot Projects Call

Securing Trust, Autonomy, and Resilience in Future Cyber Ecosystems

Call document

Publication date: 15th June 2026
EOI required by: 13th July 2026, 4:00pm UK time
Closing date: 31st July 2026, 4:00pm UK time

Item	Details
Funders	CRANE, under EPSRC Grant EP/Z534845/1
Funding type	Pilot research projects
Total funding available through this call	Up to approximately £580,000
Maximum project value	Up to £62,500 full economic cost (FEC) of which CRANE will fund 80% (£50,000)
Smaller project values	£22,500 FEC (of which CRANE will fund £20,000) £12,500 FEC (of which CRANE will fund £10,000)
Project duration	Up to nine months
Expected project start	October to December 2026
Expected project end	April to June 2027
Submission route	EOI: Submit your EOI before 13th July 2026 via: this link. Full Proposal: Submission portal will be available on the CRANE website by 30 June 2026 with a submission deadline of 31 July 2026.
Contact	crane@cs.ox.ac.uk

Summary

As part of CRANE's mission from EPSRC to strengthen the UK's cyber security research community, the network is funded to support pilot research projects. CRANE is structured into three phases across its five-year term, and this is the main call for proposals in phase one. Each phase includes a *technology trends assessment* process, and the report of this for phase one will be published alongside this call. That report has informed the topics of the call, and provides more context and detail on these.

We invite proposals from researchers at EPSRC-eligible organisations for projects in the topics detailed below. Your project must put cyber security at the centre of the research and explain the security threat, vulnerability, assurance challenge, or resilience problem that it will address. Although speculative and adventurous proposals are welcome, you should consider how to ground the project in a genuine use case or practical need.

We expect to fund a portfolio of feasibility studies, pilot projects, policy-focussed research, programme grant definition work, impact acceleration activities, and development work that can shape larger future research programmes or investments. You should set out a focused,

deliverable project that can create a credible foundation for future research, translation, or policy engagement.

Your project should fall within the Frascati definition of research and should generally align with EPSRC scope. It is not expected to be at demonstrator phase or to go beyond technology readiness level 4. CRANE funds may only support activities that could be funded through a standard research grant; for example, you cannot use this funding for studentships or student costs that should normally be funded through a training grant.

Who can apply

In order to apply, you need to be a full CRANE member and employed at an organisation eligible to receive normal UKRI grant funding. You can check your organisation's eligibility online. Normal EPSRC investigator eligibility rules are relaxed, so if you are an early-career researcher you can apply, and, subject to your organisation's policies, may request funds to cover your own salary. If you are a PhD student and not employed in a research role, you are not eligible for this call. You cannot apply if you are solely based in an industrial establishment.

We are committed to equality of opportunity and encourage applications from early-career researchers. You may apply as an early-career researcher in your own right, or with a mentor where your institution requires or recommends this arrangement. More established research leaders are also welcome to apply.

You may apply as a single individual, single institution, or as a collaboration. While you do not have to include collaboration across institutions or with industry, as a Network+ we welcome well-justified academic, industry, public sector, civil society, and international collaborations where they strengthen the project and/or foster interdisciplinarity. You do not need to provide match funding, but you should identify relevant in-kind contributions, such as access to equipment, datasets, staff time, facilities, or partner expertise. In the case of a collaborative proposal, only a single application from the lead organisation is needed, and although there is no limit to collaborators, grant funds are available only to EPSRC-eligible research organisations.

Each CRANE member can lead at most one proposal submitted for this call. You can be a named investigator on at most two proposals (whether lead or not).

What we are looking for

Scope

You should propose research that directly addresses one or more CRANE priority topics and that clearly explains the cyber security challenge at the heart of the work. Your application should explain why the issue matters, why the research is timely, and what contribution the project will make beyond existing work. While proposals may focus on technical dimensions, they may also examine broader issues (such as human aspects, governance, policy, and ethics) provided they remain grounded in the context of emerging technologies.

You should also explain the intended legacy of your project. This may include a route to future EPSRC or other UKRI funding, a larger collaborative programme, an open-source artefact, a dataset, a research contribution to a policy brief, a standards contribution, a new industry or public sector collaboration, or another credible route by which the research could be translated into practice.

Call topics

The overall theme of the call is Securing Trust, Autonomy, and Resilience in Future Cyber Ecosystems. Future digital ecosystems will increasingly consist of autonomous and semi-autonomous AI systems operating across both cyber and physical domains. These ecosystems will include robotic platforms, smart infrastructure, distributed sensing systems, and fleets of cooperating cyber-physical agents, alongside AI-enabled cyber tools for software generation, monitoring, analysis, and decision-making. Such systems will evolve continuously after deployment, integrate diverse data and models, and increasingly collaborate with both humans and other AI agents. In this setting, traditional static notions of "secure-by-design" become insufficient. Future security architectures must instead be adaptive, resilient, and continuously verifiable, capable of responding dynamically to changing environments, emerging threats, and evolving system behaviour.

The following three themes give some examples of relevant research areas, but they are not intended to be exhaustive:

Trust, provenance, and AI integrity

As AI systems become embedded within critical infrastructure and organisational processes, ensuring the integrity and provenance of data, models, and outputs becomes a foundational challenge. Some possible topics in this area include methods for establishing or verifying the provenance and authenticity of AI-generated content and protecting AI training and deployment pipelines against supply-chain attacks, as well as methods for detecting manipulated, synthetic, or adversarially-generated data. Proposals might consider issues such as these in the context of ecosystems where AI systems increasingly interact with and build upon one another.

Secure cyber-physical autonomy

Robotic and cyber-physical systems are emerging as highly networked, mobile, multi-sensor platforms with large and heterogeneous attack surfaces. Service robots, healthcare assistants, and autonomous infrastructure systems raise new challenges at the intersection of cybersecurity, safety, privacy, and autonomy. Examples of topics include maintaining security and resilience of cyber-physical systems in open and potentially adversarial environments; architectures for secure communication, coordination, and data handling across heterogeneous robotic fleets; and defence against surveillance, covert sensing, and data exfiltration.

AI-augmented decision-making and human–AI collaboration

AI systems are increasingly being used to generate software, monitor infrastructure, analyse complex data streams, and support operational decision-making. As these systems become collaborative agents alongside human operators, they introduce new forms of systemic risk

and governance challenges. Key research topics include securing such systems against manipulation and unsafe behaviour; ensuring transparency, explainability, and oversight; and methods to avoid automation bias and maintain meaningful human control in collaborative human-AI workflows.

Projects may wish to address the market incentives which can be put in place for the adoption of secure products and services. This may include research on the form of such incentives, and the design principles and development practices which enable them.

Project types

You are encouraged to consider carefully the size of your project, in order to match the ambition, team capacity, and available delivery time. You should request only the resources needed to deliver the proposed work and should make the scale of the project proportionate to its objectives and outputs. Example project approaches include:

- Feasibility studies that test a new idea, method, dataset, or collaboration, or develop an evidence base for a larger future research investment proposal.
- Pilot research projects that establish evidence, prototypes at pre-demonstrator stage, methods, concepts, or evaluation approaches.
- Policy-oriented research that translates cyber security evidence into actionable recommendations.
- Impact acceleration or translation work where the research remains within the permitted scope and does not move beyond TRL 4.

The mix of investigator time (including 'buy out' etc.) and research assistant time, and other costs, is at your discretion depending on the nature of the project and your institutional policies.

Funding available

CRANE expects to distribute up to approximately £580,000 through this phase one call. CRANE may hold back or reallocate funding for other phase one opportunities, including sandpit, collaborative, international, or targeted activities. The panel may also recommend that CRANE does not award the full amount if applications do not meet the required quality threshold.

We expect the largest projects to be up to £62,500 full economic cost (FEC) of which CRANE will fund 80% (i.e., up to £50,000). Projects may request smaller amounts where this is appropriate. The indicative portfolio below shows the scale of awards CRANE expects to support, but the final distribution will depend on the quality, topic balance, and scale of applications received.

CRANE funded value (80% of FEC)	Full Economic Cost (FEC)
£50,000	£62,500
£20,000	£25,000
£10,000	£12,500

Your project must run for no more than nine months. You should plan a realistic start date between October and December 2026 and a realistic end date between April and June 2027.

We expect to fund a range of project sizes, and you should consider carefully the value for money criterion, since part-awards will *not* be offered for projects judged by the reviewers and panel as having an over-large budget for the project scope.

What you must deliver

Reporting

Grant holders will be expected to:

- Provide a brief monthly update against schedule
- Provide a final end of grant report in a format agreed with the CRANE Management Team summarising key outputs, outcomes and impacts.
- Complete a brief impact questionnaire on an annual basis for up to 5 years following the completion of the grant. You must provide information on outputs and outcomes in a form suitable for CRANE reporting and for *ResearchFish* or a successor system where applicable.
- Present the outcomes and impacts of their research to at least one CRANE seminar or All-Hands meeting and may be asked to contribute to other CRANE events as relevant.

Other outputs

Where appropriate, you should also consider additional outputs such as draft papers, open source software, datasets, evaluation materials, policy briefs, community resources, or plans for a larger funding application. You should make outputs open where this is possible and appropriate, following UKRI open access expectations and any relevant institutional requirements.

Some projects may produce confidential outputs, such as a platform grant proposal or partner-sensitive material. You should explain any confidentiality constraints in your application and propose deliverables that CRANE can evaluate and use for programme reporting.

CRANE will link the final quarterly payment to receipt of agreed deliverables.

How to apply

An expression of interest prior to application is essential (see below).

The funding application portal will be made available via the CRANE website by 30th June 2026. You should submit your application by 31st July 2026 at 4:00pm UK time. You should allow enough time for your organisation to review and approve the application before submission.

You should submit the following documents:

- a project proposal, using the word limit that applies to the amount of funding you request, including details of researcher track record;
- a financial summary using the CRANE pro forma (including a justification of resources);
- letters confirming specific external commitments where your project depends on resources, data, facilities, or partner contributions that sit outside the requested funding;
- completed institutional agreement letter

You should not include general letters of support that do not provide specific commitments.

Indicative proposal content

Your proposal may use a free format, but you should address the following points clearly and directly:

1. the cyber security threat, vulnerability, assurance challenge, or resilience issue your project addresses;
2. the research question, objectives, and proposed method;
3. the novelty of the work compared with previous research;
4. the fit with one or more call topics;
5. the expected outputs and deliverables;
6. the prospects for translation into practice or for development into a larger research programme;
7. the team, roles, and any in-kind contributions;
8. the project management plan, timeline, and key risks;
9. your approach to responsible innovation, diversity and inclusion, trusted research, and ethics where these are relevant to the research or the team recruitment.

Word limits

Your main proposal (not including the financial summary or letters) must not exceed the following word limits (including all tables, figures, references, etc.)

Requested CRANE funded value (80% of FEC)	Project proposal limit
Up to £10,000	Up to 1,500 words
Up to £20,000	Up to 2,500 words
Up to £50,000	Up to 4,000 words

Responsible Innovation

You should identify ethical issues, data protection considerations, security sensitivities, dual-use risks, trusted research considerations, and any institutional approvals that your project may require. You should explain how you will manage these issues within the proposed timeline, taking account of the timescales of institutional ethics committees or other approval processes. You should also explain any diversity and inclusion issues which may arise with your research and how they will be addressed.

Process and Deadline

Expression of Interest

If you expect to apply for funding, you must submit an expression of interest by Monday 13th July 2026 at 4.00pm UK time. The EOI will ask for:

- names and institutions of all proposers
- project title
- topic keywords
- indicative total budget range (up to £10,000, up to £20,000, up to £50,000)

This will help us to expedite the review process after the full proposals are received. For this reason, no changes to these details will be allowed between EOI and full submission.

Link to EOI submission portal

Full proposals

Applications must be received by Friday 31st July 2026 at 4.00pm UK time. We are unable to consider late applications or make amendments to applications once submitted.

How to submit: A link to the proposal submission portal will be published on our website by 30th June 2026. Note that the proposal system does not offer the ability to save your work and return to it later. You are advised to prepare your submission elsewhere, and upload it as a final step. Institutional agreement (including agreement with the award pro forma terms and conditions) will be needed, and a template letter for this is provided. This should be signed by a responsible officer of your institution – whoever is normally responsible for approving proposal submissions to EPSRC/UKRI.

Outcome

We expect to advise you of the outcome by Friday 11th September 2026.

How we will assess your application

Review process

CRANE will recruit a reviewer college from its membership, including associate members where appropriate. CRANE may recruit reviewers through open application, nomination, or direct invitation. Membership of the reviewer college does not prevent you from applying to the call, but CRANE will manage conflicts of interest through the submission and review process.

An award panel will consider applications after review. The panel will be drawn from the CRANE leadership team and Community Advisory Board and may overlap with the reviewer college. You may not submit an application if you are a member of the award panel. Panel members will leave the discussion for applications from their institution and for any other actual or perceived conflict of interest.

CRANE will apply confidentiality and process norms broadly consistent with EPSRC practice. The panel will rank applications by overall quality, identify applications that are not fundable, and consider topic balance across the portfolio. If applications are otherwise tied, the panel may resolve the tie in favour of early-career researchers.

The panel may recommend funding, not funding, partial funding, or revisions to particular proposals. The panel will act with fairness and transparency, but CRANE will retain discretion over final funding decisions and may decide not to award all available funds.

Use of AI Tools

You may use AI tools in creating your proposal, but you remain responsible for the content, scope, and feasibility of the proposal you submit. You will need to have regard to confidentiality when using certain AI tools.

We may use AI tools in initial assessment of proposals, but reviewers will be accountable within CRANE for their reviews, and final ranking decisions will be made by the members of the award panel. Any use of AI tools will be consistent with CRANE's obligations of confidentiality with regard to your proposal.

Assessment criteria

Reviewers and panel members will assess applications against the following criteria:

- Fit to the call: the project puts cyber security at its centre and aligns with one or more call topics.
- Research quality and novelty: the project asks a clear question, uses an appropriate method, and makes a contribution beyond existing work.
- Importance of the threat or challenge: the project explains the security problem and why it matters to future technologies, practice, policy, or research.
- Deliverability: the workplan, team, resources, governance, and timescale are realistic for a project of the proposed size.
- Outputs, translation, and legacy: the project identifies credible outputs and a plausible route to future research, adoption, policy influence, or community benefit.
- Value for money: the requested resources are justified, proportionate, and aligned with the expected outputs.
- Responsible research: the project addresses diversity and inclusion, ethics, trusted research, security sensitivities, and responsible innovation where relevant.

Award terms and conditions

Standard award terms are published alongside this call. These terms are derived from and generally consistent with EPSRC terms. When submitting an application, your institution must agree explicitly to those terms.

CRANE will confirm award management, reporting, payment, data management, publication, intellectual property, confidentiality, and acknowledgement requirements in the final award terms. You should ensure that your research office or equivalent institutional authority has reviewed the terms before submission.

Timetable

Date	Activity
1 June 2026	Advance notice sent to the CRANE community
15 June 2026	Call issued ahead of the CRANE All-Hands meeting EOI portal open (via CRANE system)
no later than 30 June 2026	Submission portal open
13 July 2026, 4:00pm UK time	Expression of interest deadline
31 July 2026, 4:00pm UK time	Call closes and review begins
First or second week of September 2026	Prioritisation panel
October to December 2026	Projects begin
April to June 2027	Projects end

Contact

For questions about the call, contact the CRANE team at crane@cs.ox.ac.uk. For questions about your institution's approval process, costings, or internal submission deadlines, contact your research office in the first instance.

Privacy Notice

CRANE will collect some personal information in order to manage and process your funding application. Personal data will be handled in line with GDPR requirements. We will treat proposals as confidential and share only with the CRANE Management Team and peer reviewers.

A record of the decision-making process will be kept until the three months after the end of the CRANE grant (March 2030). For details of how CRANE handles Members' data more generally, see our Privacy Policy.

Summary of Call Documents

- This call document
- Award Terms and Conditions
- Institutional Support *pro forma* letter
- Financial Summary *pro forma*

The CRANE technology trends report is intended to be published alongside this call, and to be read in conjunction with it, but is not part of the call.