National Cyber Security Centre, in Collaboration with the Research Institute in Trustworthy Inter-connected Cyber-physical Systems (RITICS)

"NIS Directive": Call for Proposals

Closing date: Friday 8 June 2018, 16:00

Summary

The National Cyber Security Centre (NCSC), working in collaboration with the Research Institute for the Trustworthy Inter-connected Cyber-physical Systems (RITICS), is inviting proposals from academic researchers for research into the topic of the impact of the Network and Information Security Directive.

Working in conjunction with NCSC whilst undertaking research which is published in the public domain, RITICS has a strong track record of delivering high-quality academic research with the potential to significantly improve the field of cyber security, particularly in the field of operational technology (OT) or, more generally, cyber-physical systems. The RITICS community is multidisciplinary in nature, and includes a significant number of stakeholders in cyber security for OT practice, drawn from across government and industry. The successful project will form part of the RITICS community, and will share its research outputs and join in community events.

Background of the Research Institute in Trustworthy Inter-connected Cyber-physical Systems (RITICS)

RITICS was founded in 2014, as the third of the cyber security Institutes set up by the UK Government in conjunction with the Engineering and Physical Sciences Research Council (EPRSC). Its early focus was to improve Cyber Security of Industrial Control Systems. RITICS was renewed and relaunched in spring 2018, with funding for a further 5 years, now sponsored by the National Cyber Security Centre in partnership with EPSRC.

The vision is that RITICS will carry out high-quality research which advances knowledge in research areas identified as having the greatest potential to transform the academic state of the art and user practice. In addition, it is anticipated that RITICS will provide a focus for liaison with stakeholders from the NCSC and other parts of government and business.

EPSRC and the NCSC aspire to promote wide visibility of the outputs of RITICS in order to enable fast dissemination and, where appropriate, application of the research to improve Cyber Security of cyber-physical systems and critical infrastructure in the UK as a whole.

NIS Directive Theme

The UK will be implementing the EU directive on the security of Networks and Information Systems (known as the NIS Directive). Network and information systems and the essential services they support play a vital role in society, from ensuring the supply of electricity and water, to the provision of healthcare and passenger and freight transport. Their reliability and security are essential to everyday activities.

The EU recognised that any cyber security incident could affect a number of Member States and in 2013 put forward a proposal to improve the EU's preparedness for a cyber attack. This proposal became a directive in August 2016, giving Member States 21 months to embed the Directive into their respective national laws.

As we have seen from numerous cyber security incidents these systems can be an attractive target for malicious actors, and they can also be susceptible to disruption through single points of failure. Incidents affecting any of these systems could cause significant damage to the UK's infrastructure, economy, or result in substantial financial losses. The magnitude, frequency and impact of network and information system security incidents is increasing. Events such as the 2017 WannaCry ransomware attack, the 2016 attacks on US water utilities, and the 2015 and 2016 attacks on Ukraine's electricity network clearly highlight the impact that incidents can have.

There is therefore a need to improve the security of network and information systems across the UK, with a particular focus on essential services which if disrupted, could potentially cause significant damage to the economy, society and individuals' welfare.

Context for the research

The research will address three key questions. These questions define the research challenges to be addressed by the Institute and the scope of this research. The questions are:

- What does the baseline look like currently?
- What are the challenges to the implementation of the NIS Directive?
- What are the impacts of early adoption of the requirements of the UK implementation of NIS?

Evidence proving the effectiveness or not of different options or approaches, in different circumstances, is a key output of this research. Research addressing techniques that support trustworthy information sharing is also within the scope of this call.

Other Research

Whilst only a small amount of research has been done on this topic to date in the UK and elsewhere, the intention of this initiative is to identify and build on the work that has already been done, rather than duplicating it. Similarly, there are other research initiatives that complement this work. The topic

space is large, and the intention is to align these initiatives where possible to avoid duplication of work and maximise our coverage as a community.

Research challenges

Research proposals should clearly address at least one aspect of these principal challenge areas.

1. **Establishing the baseline.**
   The main outcome from this work should be an understanding of current best practice in the affected sectors of UK industry, both within each sector and cross-cutting. This may be achieved through literature studies and field studies with key industrial partners. It will also be important to understand the current baseline in other major European countries and in other countries such as the US.
   In some sectors, the relevant Lead Government Department may already expect a certain baseline or have specific targets. The project should take account of this.
2. **What are the challenges to implementation?**
   There are a number of potential challenges to implementation of the NIS Directive. These include current regulations, social/cultural barriers, the interactions between safety and security, economic and technological constraints. Approaches could involve sociological studies, formal modelling to understand the impact of certain approaches and other techniques.
   The Directive requires organisations to share information with NCSC. There may also be benefits in sharing information with other organisations in the same sector as already happens in the finance sector. This is likely to require research into new techniques for overcoming some of the concerns over information sharing, particularly legal, confidentiality and minimum necessary disclosure issues.
   The foregoing is not intended to be an exhaustive list of possible approaches to addressing this area. Proposers are invited to consider general issues and those that might be specific to individual sectors.
3. **What are the impacts of early adoption?**
   Is the NIS Directive having the desired outcomes for the various stakeholders (Competent Authorities, NCSC – as the UK Cyber Security Authority, and other relevant bodies) of improving cyber security?
   The goal of the NIS directive is to make essential services more resilient to cyber-attack. Is the implementation having a meaningful impact and driving improvement? Is effort being directed into showing that organisations comply rather than into improvement? Has it increased spending, without meaningful improvement in cyber-security?

Research Institute – way of working

The successful project will join the RITICS portfolio, with all project staff becoming community members. Representatives from the project will be expected to attend the majority of the regular RITICS community meetings, workshops and/or conferences. The project will be asked to present its progress at some of these meetings.

There will be the opportunity to engage directly with the NCSC during the course of the project, although the majority of the interaction is expected to be via RITICS.

The project will also be expected to supply brief progress reports each quarter, and an annual progress summary, via RITICS.

What should be in the proposal?

Each proposal must make it very clear how it addresses the challenge areas described above. Proposals should also include details of any planned engagement with 'real world' security.

The proposal should specifically address each of the following items:

- Background: An outline of the context of the research.
- Aim: A description of what understanding of the topic space the research is progressing and what potential impact it will have in practice.
- Relevance to the call: A description of which challenges the research addresses, and how it addresses them.
- Data: Whether the research is planning to create or make use of any specific datasets, and how they will be generated/handled.
- Field work: Whether the research will be carried out in any 'live' environments as opposed to lab based work. Details of the trials environments should be provided and the degree to which access has been agreed.
- Resources: An overview of the timescales, resources and structure of the research. A workplan should illustrate how these aspects combine to progress the research. The resources being used should be detailed, and CVs for named and visiting researchers included where these are known. Whether the research is planning to involve any draw on any expertise from within the security community should be described, including the nature and extent of the engagement and the degree to which it has been agreed with the appropriate people/organisations in the security community.
- Method: An outline of how the research will be carried out, detailing techniques and approaches that intend to be used. An indication of the level of previous experience of these approaches should be included.
- Potential impact in practice: How the outcomes of the research will make a difference in a real-world setting.

Application submissions should be no more than eight sides of A4 and should include a breakdown of all costs involved, including equipment, travel & expenses etc. Proposals that attempt to engage with real-world partners are welcomed.

How will proposals be assessed?

Following eligibility checks, research proposals will be reviewed by an expert Assessment Panel comprising representatives from academia, industry, and HMG. The panel will produce a ranked list of proposals based on consensus scores.

The Assessment Panel will consider the following criteria:

- Quality – this will consider the method & concept for the proposed research, and its ability to move forward fundamental understanding within the field.

- Viability – this will assess how feasible the research is to carry out, eg whether the research concept is practicable to deliver. It will take into account the difficulty of the task, the logistical factors, and the track record of team.

- Significance – this will consider the research's potential impact on practice and its relevance to the Call. Note that the impact on practice does not have to be immediate. A long term, highly aspirational piece of research could produce a higher "Significance" score than a more tactical "applied" piece of work eg designed to produce an immediately usable tool. Neither does this preclude research which may have a 'negative' outcome, eg proving that a technique does not work. The proposal should outline the potential for transformative thought or progress within the cybersecurity profession, whether this be near or long term.

All three criteria will be equally weighted. However, "Significance" will have a minimum threshold, below which proposals will be rejected.

It is anticipated that a single project will be chosen for funding from this Call.

Key dates

Activity	**Date**
Call for Research Published	Late April 2018
Proposals due to be submitted	Friday 8 June 2018
Assessment Panel meeting	w/c 9 July 2018
Announcement of results and Contract Awards	w/c 16 July 2018
Research starts	August 2018

Funding available

This topic will be funded by NCSC with an indicative budget of £0.5M over 2 years. The funding and contract will be under the NCSC's standard terms and conditions: a draft copy of the contract can be made available on request. The research will be funded at Full Economic Cost. Budgets for attendance at academic conferences to publicise and disseminate the work should be included within the research

proposal. In addition to the travel budget for attending conferences, proposals should include adequate funding for travel between academic partners within the project, and to attend the quarterly Institute meetings.

The cross-disciplinary, exploratory and novel nature of the Institute is likely to require a significant commitment of time on the part of its permanent academic members.

The funders are committed to full and open publication of the research outputs of the Institute in line with normal academic practice.

Both NCSC and RITICS believe that this is a broad scale research topic, with the potential to offer significant transformative value. We will be campaigning for more attention to be given to this topic at a national scale, and seeking additional sources of funding for further research from government and industry partners.

Eligibility

Applicants need to be based in institutions eligible to apply for EPSRC funding.

How to apply

Applications should be sent to Phil Bliss, Head of GCHQ Research & Innovation Office via email: ResearchCalls@GCHQ.GSI.GOV.UK. We must receive your application by **1600 on Friday 8h June 2018.**