NSW Cyber Security Network

Research Pilot Grant Guidelines

The aim of the NSW Cyber Security network is to provide leadership and develop NSW capacity and collaboration in Cyber Security. The NSW State Government in collaboration with NSW universities, research organisations, and industry, support collaborative applied research and development to meet the State's cyber security challenges. The NSW Cyber Security Network invites applications to its Research Pilot Grants round.

Up to $1.5m will be awarded in the pilot grant round.

These guidelines provide information for applicants on the nature and scope of the grants and how to apply for pilot research funding.

Priority areas

The priority themes for the Research and Development Pilot grants are:

1. Protecting Infrastructure
2. Protecting Data
3. Protecting Industry
4. Protecting the Public
5. Building a Cyber-secure Future: Software, Hardware and Technologies

Eligibility

To be eligible for a NSW Cyber Security Pilot Research Grant, applications must be made by a Chief Investigator who is employed by one of the network’s member institutions. This includes:

- The University of NSW
- Macquarie University
- The University of Newcastle
- The University of Sydney
- The University of Technology Sydney
- The University of Wollongong
- Western Sydney University

A maximum of three proposals can be submitted as the host organization.
Collaboration

Essential

Applicants must include one or more investigators from another member institution in their application.

Industry Collaboration - Highly Regarded

Applicants are also encouraged to collaborate beyond the additional network member required.

In particular a description of how the research will be relevant to industry in the solving of end user problems.

Evaluation Criteria

Investigators and Track Record (25%)

Applicants must demonstrate the quality of their research track record and the relevance this track record has to cyber security, this project and the goal of building NSW capability in this area.

Applications must demonstrate their ability to conduct the project and must include the 5 most relevant publications for each investigator in their application.

Significance and Technical Merit (25%)

The significance of projects will be assessed in terms of its technical merit and the benefits to building NSW capacity in the area of Cyber Security and the identified priority areas.

Applicants must explain how their application will address one or more of the priorities and how this research will benefit NSW’s efforts in Cyber Security.

The areas of priority are:
1. Protecting Infrastructure
2. Protecting Data
3. Protecting Industry
4. Protecting the Public
5. Building a Cyber-secure Future: Software, Hardware and Technologies

Collaboration and Research Environment (25%)

Collaboration with other NSW Cyber Security partners is a requirement of any application to the pilot grants round. Applications not collaborating with other at least one other of the members will be ineligible.
Partnerships may be based on new or extend existing activities. Applicants must explain how their partners are critical to the project, why the partnership is needed, and detail the role each partner will undertake in the project.

Applicants must address how their research environment and its collaboration with other members will facilitate the successful completion of the project.

**Industry Relevance and Future Leveraging (25%)**

Applicants are also encouraged to collaborate beyond the additional network member required. In particular, a description of how the research will be relevant to industry and in solving end user problems. Collaboration with industry is not essential but highly regarded.

The pilot grants aim to seed larger research funding and collaboration opportunities. Applicants must identify how the seed fund will be leveraged to develop the collaboration and plan for future larger - scale projects. Including:

1. Potential future industry partners needed in the project
2. Potential future funding sources that will be attracted to the project.

The research project must explain the opportunity for the work to be leveraged through industry needs, partnerships and funding opportunities.

**Budget and Value for money**

Address how the project budget represents value for money to NSW and how it will effectively be used to build capacity in NSW cyber security.

**Due Date**

5pm 30 May 2018

No extensions will be approved.

PDF Format emailed to andrew.johnson@nswcybersecuritynetwork.com.au

**Assessment**

**Step 1**

Applications will be examined by members of the steering committee to ensure that all partners are included in the decision-making process. The steering committee will comment on the proposals against the criteria and pass them to the independent panel for assessment. Applicants cannot review their own submissions.
Step 2

An independent panel will assess and rank the applications. This panel will include at least the Chair of NSW Cyber Security Network, NSW Cyber Security Network Director, NSW Government, Data61, Cyber Security Growth Centre and a cyber security industry representative. In making its recommendations this group will take into account the strategic imperative for proposals, a balanced approach across member Universities and Network priority areas.

Level of Funding

Grants are expected to be funded between $50,000 - $150,000 each. Grants of significant merit including large-scale collaboration with multiple members may attract a higher amount of funding.

Duration of funding

Funds must be used within 12 months from the date of award.

Ineligible expenditure

Expenditure from the pilot grant cannot be used to pay part or the full salary of the Chief Investigator. Expenditure would normally be limited to the standard research costs eg research assistance, travel and accommodation, minor equipment and software.

Intellectual Property

Any intellectual property developed from the research will accord with the IP arrangements established in the network agreement. Section 11 of the Network agreement requires:

that NSW is provided a perpetual, transferable, royalty free licence (including a right to sublicense) to use the IP in the Project Material. Each party retains ownership of any material or Background IP it provides to enable the Services to be carried out. And that each Party grants to the other party a worldwide, free, perpetual, irrevocable, nonexclusive licence to use the Background IP the granting party provides (including a right to sublicense the Background IP) for the purposes of this Agreement, for internal research and education.

Publications and Media

In applying for this funding you acknowledge that if successful you agree to acknowledge NSW Government and its support in:

(a) in any public statements about the Network;
(b) on the home page of any website established in connection with the Network
(c) you must use the Department’s logo when acknowledging the Department’s support of the Network as the Department directs, in accordance with relevant Departmental guidelines and the NSW Government Branding Style Guide as set out at http://www.advertising.nsw.gov.au/sites/default/files/downloads/page/nsw_government_branding_guide.pdf
NSW Cyber Security Network

Addendum

Key Industry Challenges

Challenges

The NSW Cyber Security Network has been established to support the development of NSW research and industrial cyber security capacity. In establishing the network NSW and most of its universities are seeking to provide leadership in the development of the states’ capacity to respond and build economic opportunity for NSW businesses focused on cyber security.

Increasingly challenges to industry are being responded through rapid responses to challenges that confront industry and government. Organisations are relying less on internal R&D capacity and seeking support to their challenges through entrepreneurial innovation platforms drawing on substantially larger research capacities found in nimble SME’s and start-ups, universities and public industrial research organisations.

The NSW Cyber Security Network seeks to facilitate the development of the state’s capacity in cyber security by funding a challenge round and promoting the collaboration between NSW research and business communities.

End users in the public, private, for profit and not for profit sectors are encouraged to bring forward their cyber security challenges for the promotion of solutions through funded projects through NSW research capabilities.

1. Personal Travel Data

Challenge Summary:
Describe the challenge in less than 20 words
Data from cars is currently being collected by motor vehicle manufacturers, ride-sharing companies (UBER, hire cars and rental), mapping companies and the State Government.

Summary of Challenge
Describe a summary of the challenge in less than 200 words. Include a summary of the challenge and the anticipated outcomes.
This data is personal information and is not freely available to the owner and is being used by these companies without the explicit consent of the owner or consumer. Autonomous vehicles will increase the data being generated as well as data ‘going off shore’ with increased connectivity and autonomy.

Opportunities:
- NSW to lead the conversation on personal travel data with possible regulatory measures
Mitigation strategies for companies to prevent data breaches
Wide range of stakeholders

Stakeholders:
- NSW Government
- NRMA
- UBER
- Google
- Car manufacturers
- Insurance retailers
- Partner Universities

Possible research areas:
- Trust
- Governance
- Network security
- Machine Learning
- Policy
- Blockchain
- Cryptography
- Secure operating systems

Research Collaborators:
- USyd (inc Australian Centre for Field Robotics) (Network Security)
- WSU (Trust and Governance)
- UoN (Cloud Security and Infrastructure Security)
- Maquarie University (Data Analytics)
- UNSW (Network security)
- UoW (Cryptography)
- UTS (Machine Learning)

2. Water Utilities
Challenge:
Describe the challenge in less than 20 words
Water Utilities are moving towards smart meters and the collection of Data to inform their business decisions, drive efficiencies and become more competitive.

Summary of Challenge
Describe a summary of the challenge in less than 200 words. Include a summary of the challenge and the anticipated outcomes.
Initiatives such as smart meters are being trialed and are creating large amounts of Data (Big Data) and an increasing need to develop new technologies to develop efficiencies in the delivery of their product.

Opportunities:
Working with key NSW Utilities to assist in ensuring that their Cyber capabilities are at the forefront of technologies and are driving efficiencies.

**Stakeholders:**
- Sydney Water
- Hunter Water
- NSW Cyber Security Network
- Partner Universities

**Possible Research Areas:**
- Network Security
- Cryptography
- Trust
- Governance
- Secure Operating Networks

**3. Penetration Testing (Ethical Hacking)**

**Challenge Title:**
Describe the challenge in less than 20 words
Industries and Government departments need to undertake penetration testing to see how robust their on-line components of their business are and how safe they are from Cyber attacks.

**Summary of Challenge**
Describe a summary of the challenge in less than 200 words. Include a summary of the challenge and the anticipated outcomes.
All industries and agencies and interested in and are undertaking to some level penetration testing. Testing is generally done via a commercial agent with bigger business having a number of penetration tests being undertaken by a number of businesses on a range of issues.

**Opportunities:**
Collaboration with a wide variety of industries with a high level of student engagement in meaningful projects. Engagement with a majority if not all partner Universities in meaningful Industry focused projects.
This testing gives a low risk, confidential way of running projects for a wide range of instrumentalities and students.

**Stakeholders:**
- Bug Crowd
- NSW Cyber Security Network
- Partner Universities
- Industries
- Government Departments
**Possible Research Areas:**
- Cryptography
- Network Security
- Trust
- Governance
- Blockchain
- Secure operating systems

**Research Collaborators:**
- All

4. Hunter Valley Coal Chain Coordinator (HVCCC)

**Challenge Title:**
Describe the challenge in less than 20 words

A) Threat Analysis and Risk Analysis
Assistance required to:
- Analysis of HVCCC’s risk profile from an external perspective including identification of external threat actors, attack vectors and potential mitigating controls
- Review of HVCCC’s internal security controls and processes to identify risks
- Development of a detailed security roadmap for HVCCC bases on the internal and external assessment.

B) Zone based Firewall Areas
Assistance required to:
HVCCC is looking to move to a policy driven multi-zone firewalled DMZ environment to improve security and simplify firewall management. Key principles would include;
- Production separated from test/development environments.
- Policy driven firewalls to minimize complexity of firewall configuration/auditing e.g. A database server in an internal DMZ, could push information to a database server in an external DMZ but not the reverse.

The requirements include a review of HVCCC’s current network/firewall design and a proposed model and firewall policy for the target state.

**Summary of Challenge**
Describe a summary of the challenge in less than 200 words. Include a summary of the challenge and the anticipated outcomes.

**Opportunities:**
Working with the key logistics body for one the key economic drivers in the State on a specific Cyber task. If something happens to HVCCC there is a big problem for industry and the Government.

**Stakeholders:**
- NSW Cyber Security Network
- HVCCC
• Partner Universities

**Possible Research Areas:**
- Governance
- Secure Networks
- Policy
- Governance
- Secure Operating Networks

**Research Collaborators:**

5. **NSW Government Department Cyber Security Framework**

Challenge Summary:
Describe the challenge in less than 20 words
NSW Government departments are looking to develop a Cyber Security framework and policy to mitigate possible risks.

Summary of Challenge
Describe a summary of the challenge in less than 200 words. Include a summary of the challenge and the anticipated outcomes.
The NSW Auditor General has recently handed down a report and has strongly recommended that Government departments need to develop mitigation strategies for Cyber risks.

**Opportunities:**
To assist in developing a NSW Government Cyber framework.

**Stakeholders:**
- NSW Government (Finance and Innovation, NSW Govt CIO initially)
- NSW Cyber Security Network
- Partner Universities

**Possible Research Areas:**
- Governance
- Trust
- Secure Networks
- Policy