Australian Academy of Science
National Committee for Information and Communications Sciences

Response to the Draft Science and Research Priorities for Australia

March 20, 2015

The Australian Academy of Science National Committee for information and Communication Sciences has examined the document entitled "Draft Science and Research Priorities for Australia" issued by the Chief Scientist's Office on March 18, 2015 and offers the following comments and recommendations:

Comments:

1. In the draft document, the focus of the draft Cybersecurity priority area is restricted to security issues related to malicious attacks and cyber crime. In the view of the National Committee for Information and Communication Sciences, this focus is much too narrow. It ignores the wider and perhaps even more important issues of security of cyber infrastructure under threats of poor hardware and software reliability, natural disasters, human error, and other unforseen events. The National Committee considers it essential that this priority area have a broader focus because:

    a. Malicious attacks can exploit weaknesses in cyber infrastructure due to undesirable but non-malicious events. In other words, a network optimized for defence against malicious attack might be vulnerable to non-malicious events, and vice-versa. It is good network engineering to consider these optimizations jointly. From a scientific point of view, joint optimization is needed if new and innovative outcomes are to be obtained.

    b. A unified approach to malicious and non-malicious security provides unique opportunities for Australia to lead the world in innovative and potentially commercially valuable research.

    c. Australia is developing an increasing dependency on cyber infrastructure, and the security of this infrastructure in all eventualities is essential. Security during bushfires, floods and cyclones are three examples.

    d. A broader focus in this priority area provides much better synergies with other priority areas, through the development of secure cyber infrastructure technologies that support those other priority areas. In short, a broader focus will provide much better outcomes for Australia.

2. To a varying degree, there is some acknowledgement of the importance of information and communications technologies (i.e. cyber infrastructure) in the text and three focus points in each of the priorities. But the potential impact of ICT in furthering Australia's national R&D

agenda is understated in the document. The National Committee for Information and Communication Sciences believes that new secure cyber infrastructure will have the potential to transform the practical implementation of developments in all of the priority areas. Examples include:

a. Transport: Automated technologies, such as collision avoidance, cooperative vehicle highway systems, telematics for transport with zero fatalities, reduced emissions and congestion through real-time data analytics.

b. Food: Sensor networks, localisation technologies, data bases and software enabled automated remote sensing of agricultural products, gathering and sharing of information on food security, authenticity, improve hazard management and food quality.

c. Climate Change: Gathering information on climate change through advanced ICT applications, Real-time data analysis and communication Data driven modelling of future impact of climate change on food production, health, disaster incidence and design of adaptation strategies

d. Energy: Data driven automated Australian grids

3. In short, the National Committee on Information and Communication Sciences feels that significant opportunities will flow from a close linkage between a broadened Cypersecurity priority and other national priorities where ICT will have an positive impact.

Recommendations:

The Academy of Science National Committee on Information and Communication Sciences recommends that

A. The relevance of ICT in all research priority areas be spelled out more clearly, and potential synergies between the ICT roles in each of the priority areas be identified,

B. The Cybersecurity priority area be re-focussed on a broader integrated approach to security, and resilience in the face of a wider range of threats, and that linkages to other priority be highlighted,

C. The text for Cybersecurity, in the document released by the Chief Scientist's Office is re-drafted along lines in the Appendix below. In the suggested text in the Appendix we have:

a. Changed the term "cyberspace" in the original text to "cyber infrastructure" the NCICS feels that this a more appropriate term, for a number of reasons
b. Broadened the focus of the priority area to include more aspects of security.
c. Restructured the three highlight areas to align with the broader focus, and to provide explicit links to the other priority areas.

Appendix:

Recommended re-drafted text

4. Cybersecurity
Australia's cyber infrastructure underpins the entire knowledge economy, including government, business, defence, police, and emergency services. But our cyber infrastructure is vulnerable to exploitation by malicious actors and is subject to damage caused by non-malicious events such as natural disasters, equipment failure, human error and other accidents. It is essential that the security and survivability of this key infrastructure is assured. Research in cyber security will position Australia as a leader in fast moving and emerging areas such as distributed network management and the internet of things, machine learning, and intelligent and secure data management and retention.

Departments and agencies should give priority to research that will lead to:

1. highly-secure and resilient communications and data acquisition storage retention and analysis for government, defence, business, emergency services, transportation systems and health services.
2. secure, trustworthy and fault-tolerant technologies and software for improved food production, environmental monitoring, logistics, transportation, smart grids, and public health.
3. new technologies for detection and monitoring of vulnerabilities in cyber infrastructure and for managing recovery from failure.