

## **Reporting Responsibilities of the ARC Research Networks**

The Funding Agreement for ARC Research Networks for funding commencing in 2004 requires administering organisations to provide two components of reporting:

- Annual Report; and
- End of Year Report

### **Annual Report:**

Attachment 1 describes reporting requirements that are based on the Research Networks Funding Agreement. It includes Attachment 2 which is a menu of Performance Indicators that might assist Network Convenors/Administrators in providing their Annual Reports.

Attachment 3 is a Financial Statement proforma. This must be completed and forwarded with the Annual Report.

### **End-of-Year Report:**

A spreadsheet template was forwarded by the ARC to host institution Research Offices for each scheme in mid-January 2006.

The first Annual and End of Year Report covering the period from the commencement of funding until 31 December 2005 are due on **31 March 2006**.

Both the Annual Report and the Financial Statement should be forwarded to:

The Executive Director  
ARC Research Networks  
Australian Research Council  
GPO Box 2702  
CANBERRA ACT 2601

Annual Report

The Annual Report should be set in the context of the Research Network's overall goals and objectives, programs and research priorities, performance indicators outlined in the application (or subsequently developed), activities and strategies. It should report on the operation of the Research Network in accordance with the Approved Proposal, the Funding Agreement and the Funding Rules for Research Networks for funding commencing in 2004.

The following information must be included in the Network's Annual Report:

- A summary of the overall goals and objectives, programs and research priorities and any changes to these that may have occurred during the past year;

The overall goals and objectives, programs and research priorities for Research Network for a Secure Australia (RNSA) have not changed during the past year. The RNSA remains committed to its original aim to create a multi-disciplinary collaboration to strengthen Australia's research capacity and enhance the protection of the nation's critical infrastructure from natural, human-caused, or accidental disasters, and terrorist acts.

The RNSA this past year, has been successful in its goal to establish a research network primarily under the National Research Priority 4 –Safeguarding Australia: Priority Goal 1 – Critical Infrastructure Protection (CIP). This goal also includes some elements from other national priority areas, such as frontier technologies, advanced materials, smart information use, transformational defence technologies, and protecting Australia from terrorism and crime.

The RNSA has been able to bring together the majority of Australia's leading researchers, government and industry leaders involved in CIP. As well, the RNSA has been able to facilitate a knowledge-sharing network for research organisations, government and the private sector to develop research tools and methods to mitigate emerging safety and security issues relating to critical infrastructure. The network has also been able to integrate complementary, yet diverse research areas including physical and information infrastructure security, and surveillance and intelligent systems.

The Australian government has identified the need to secure critical infrastructure against potential natural or human-caused disasters including terrorism as a national priority. The RNSA has endeavoured in the past year, to meet this important government requirement through providing research coordination in the areas of CIP.

The RNSA continues to receive strong support from key government organisations responsible for Australia's CIP and Counter-Terrorism (C-T) such as the Critical Infrastructure Advisory Council (CIAC), the Attorney-General's Department, Trusted Information Sharing Network (TISN) for Critical Infrastructure Protection, the Department of Prime Minister and Cabinet – National Security Division (SET Unit) and Emergency Management Australia (EMA).

- The extent to which the objectives of the Research Network and the Approved Proposal have been met;

The objectives of the RNSA have been fully met with the inclusion of 160 of Australia's leading researchers in CIP from universities, government and industry. These researchers are currently involved in a wide ranging series of collaborative workshops, seminars and an annual conference program designed to achieve research collaboration, nationally and internationally.

- The achievements of the Research Network, Network Participant contributions to the Research Network and other outputs achieved resulting from the use of the Funds, including any advances in knowledge, relevant publications, or international collaboration. Networks should report on all aspects of importance to their particular area of research and environment, and may select from the menu of reporting items/performance indicators (Attachment 2) that may be relevant to their particular Network, noting that the menu list is not inclusive;

A number of significant contributions to the RNSA in the past year have been noted:

- The RNSA Focus Group Meeting and Launch (24<sup>th</sup> February 2005) at Australian Defence Force College and Parliament House, Canberra. The Attorney-General, Mr. Phillip Ruddock launched the network at Parliament House. In addition Mr. Gary Nairn, Parliamentary Secretary to the Prime-Minister represented the Minister of Education. Other speakers included the Head of the SET Unit, Dr. Lynn Booth and ARC Executive Director, Prof. Elim Papadakis. Over 119 leading academic, government and business leaders in the CIP area attended this event.
- Safeguarding Australia conference, 14<sup>th</sup> July 2005, including the SET Summit on counter-terrorism technology. Over 300 people attended the event in Canberra. All three days of the event highlighted the contribution that science, engineering and technology can make to national security, either directly or indirectly. The proceedings - Recent advances in counter-terrorism technology and infrastructure protection, was produced and this contained the refereed papers from the summit. These proceedings have now been published - Mendis, P; Lai, J; Dawson, E. (Eds.). *Recent Advances in Counter-terrorism Technology and Infrastructure Protection*. ISBN: 0975787314 – and are providing an important source of publicly available information on CIP in Australia today.
- The organizing of 19 other seminars, workshops and collaborative research discussion and focus groups, namely:
  1. Security Seminar, Roxanne Zolin, Naval Postgraduate School. Held in Canberra, at UNSW @ ADFA (2 February 2005);
  2. Engineering Security Research Forum. Held in Canberra, at UNSW @ ADFA (25 February 2005);
  3. Centre of Excellence for Risk Analysis, talk by Prof Jean Cross, UNSW, Held in Canberra, at UNSW @ ADFA (14 June 2005);
  4. PhD workshop on Counter-Terrorism, Critical Infrastructure Protection and national security. Held in Canberra, at the Australian National University (15 June 2005);
  5. The 10th Australasian Conference on Information Security and Privacy (ACISP 2005). Held in Brisbane at the Information Security Institute, Queensland University of Technology (4-6 June 2005);
  6. RNSA Networks Workshop on Research Challenges in Information Security. Held in Brisbane at the Information Security Institute, Queensland University of Technology (7 July 2005);
  7. Half day seminar, “understanding tsunami threat to Australia and mitigation technologies”, June 2005.
  8. RNSA Workshop on Computer Forensic. Held in Brisbane at the Information Security Institute, Queensland University of Technology (8 July 2005);

9. RNSA Workshop on Location Based Security: GPS , future GNSS and their use in Critical Applications, Held in Canberra at UNSW @ ADFA (8 July 2005);
10. Security Seminar: Mike Rothery Assistant Secretary, Critical Infrastructure Protection Branch, Australian Government Attorney General's Department, "Critical Infrastructure Protection - Allowing business leaders to make informed decisions about risk", Held in Canberra, at UNSW @ ADFA (2 August 2005);
11. RNSA Seminar: Mr. Athol Yates, Australian Homeland Security Research Centre, Australia, "Is it millions or billions? Defining the size and direction of the new national security market", Held in Canberra, at UNSW @ ADFA (7 September 2005);
12. ID Security: Trends, Current Technology and Future Directions, Held in Canberra (8 September 2005);
13. Security Seminar: Prof David Hill ARC Federation Fellow, Research School of Information Science and Engineering, ANU, "Global Security Control of Power Systems". Held in Canberra, at UNSW @ ADFA (28 September 2005);
14. Counter-Terrorism Seminar & Workshop: Dr Chris Flaherty "RNSA Counter Terrorism Capabilities", NSW Police Crime Prevention Conference. Held in NSW Police College, Goulburn, NSW (27 September 2005);
15. Intelligence CCTV: Trends, Current Technology and Future Directions. Held in Canberra (4 October 2005);
16. 1<sup>st</sup> Colloquium for Information Systems Security Education – Asia Pacific (CISSE-AP), Held in Adelaide, 21-22 November 2005);
17. Risk Assessment Workshop. Held in UNSW, Sydney (28-29 November 2005);
18. Counter Terrorism Closed Session Workshop. Held in UNSW, Sydney (28-29 November 2005);
19. Blast Effects Design/Analysis Short Course. Held in University of Western Australia, Perth (5-6 December 2005).

- Any contributions to the Research Network of particular significance during that year;

Several key achievements of the RNSA, in particular:

- Support from the Attorney-General, Mr. Phillip Ruddock, and his departmental officers in the Critical Infrastructure Protection Branch. This has included chairing the RNSA Advisory Board, and access to the CIP Branch Newsletter, allowing articles reporting on RNSA activities to be published. This publication is circulated to all branches and levels of the Federal and State governments involved in CIP areas, and this has significantly raised the research profile and credibility of the RNSA professionally within Australian government.
- Participation in the development of a CRC application (CRC-SAFE) for current round of submissions, seeking funding under National Research Priority 4 –Safeguarding Australia: Priority Goal 1 – Critical Infrastructure Protection (CIP). This application is supported by a broad based consortium of university, government and industry. This activity has significantly mobilised Australian CIP research and industry support and engagement with this research.
- The RNSA has been successful in promoting leading researchers to take a leading role in organising opportunities for collaborative CIP research in Australia and internationally. In particular, these research leaders have undertaken the following activities:

1. A Counter-Terrorism collaborative research group has been formed within the RNSA (webpage <http://www.secureaustralia.org/ResourcesAndLinks/ct.php>). This has been a significant development using the RNSA as a vehicle for achieving a national agenda in Australian C-T research. To that end, a number of significant gains have been made over the last few months. In particular, the RNSA has assisted with the formation at Macquarie University of a Centre for Policing, Intelligence and C-T; and played a key role in the development of ECU's Centre for Counterterrorism, Security and Intelligence, which will be offering Australia's first full degree Bachelor of Counterterrorism, Security and Intelligence
  2. The RNSA has also established collaborative C-T research links with Imperial College, London; Resilience Centre, Royal Military College of Science, Cranfield, UK; and the Italian Agency for New Technology, Energy and the Environment. A number of special C-T collaborative research workshops have been organised that have enabled researchers and end-users to identify gaps in C-T research within Australia.
  3. The RNSA has formed a research group on risk and security. The group (led by Dr Tony Green (UNSW); Prof. Jean Cross (UNSW); A/Prof Colin Duffield (UniMelb); and Dr Collette Burke (RMIT) has taken a leading role in identifying the gaps and research needs in risk related to Australian CIP. The major output from this group, has been the holding of a workshop for risk and security, in November 2005. This was a highly successful start to the process of developing collaborative research in the risk area. Some 70 risk experts were brought together for this event, forging closer links. This has produced some outcomes that can be worked on for the future. A copy of the workshop report can be found on the RNSA website at <http://www.secureaustralia.org/NewsAndEvents/riskworkshop.php>
  4. The development of the RNSA Collaborative Research Group for Facility Hardening currently conducts research applied to improving the security of facilities based on integrated cohesive and effective 'all hazards' approaches. See <http://www.secureaustralia.org/ResourcesAndLinks/hardening.php>
  5. A research group on human factors led by Prof. Lynn Batten (Deakin Uni) and Dr. Katina Michael (Uni Wollongong) has been formed to develop human factors collaborative research in the context of implications for information and engineering. A Social Implications Workshop is organized for 29th May 2006 at University of Wollongong. This will provide attendees with the opportunity to network and learn about the current and potential status of information security measures, to consider their implications on citizens and business, and to identify their impact on legislation and privacy at both a local and global level.
- Since February 24<sup>th</sup>, 2005 (the launch of the RNSA in Canberra), the RNSA has gained 160 Network Participants (until 31<sup>st</sup> Dec. 2005). Many others have joined since January 2006.

- The Register of Participants, current up to the date of the Annual Report;

See Attachment 4

- Contribution to the National Benefit;

The Australian government has set as a national priority the need to secure critical infrastructure against potential natural, human-caused disasters, accidental or terrorist acts. The RNSA has sought to create a knowledge-sharing network for government, universities and the private sector, producing innovative solutions to secure Australia's CIP

from threats that have potential for causing significant national security, economic, and/ or social impacts.

The RNSA has facilitated a coordinated approach to CIP by aligning the efforts of researchers and key stakeholders from government organisations and the private sector in the broad areas of science, engineering and technology. The network also serves as a vehicle for the dissemination of best research practices in CIP, as well as a repository of expertise to advise government and industry on CIP matters.

The RNSA has developed strong links with a number of leading research agencies, university research groups, CRCs, government organisations and industry. Together these have tailored a CIP research agenda meeting Australia's needs. In particular, the RNSA has been a valuable asset to the Federal Government's TISN structure by providing to both its CIAC (Critical Infrastructure Advisory Council) and its associated EAGs (Experts Advisory Groups) appropriate R&D insights into fundamental and applied CIP issues. In support of which, the RNSA has already established and will continue to establish notable contacts and collaboration with equivalent or similar activities overseas, e.g. in Europe, Asia, USA, Canada, and NZ. The RNSA activities program and its outreach plan foster the development of local expertise through the enhancement of postgraduate education and the encouragement of CIP researchers, having particular emphasis on cross-disciplinary approaches. The overall aim of these activities has been to ensure that security advice in relation to CIP will not need to completely depend on imported or overseas skills.

- An indication of the activities and strategies for the coming year; and

The RNSA will continue to facilitate collaborative research on policy, business decisions, analysis techniques, and treatment options in order to secure Australia's critical infrastructure. The network will continue to establish integrated research programs enabling collaborative research relationships. The network will launch activities programs (workshops, focus groups, summer retreat, and an annual conference) throughout each year, to foster research collaboration and nurture young investigators. In particular, the RNSA has developed the following events:

- Counter-Terrorism collaborative research workshop 24<sup>th</sup> February, 2006, University of Melbourne. will provide attendees with the opportunity to network and learn about the current research development in the C-T area.
- Social Implications Workshop (29<sup>th</sup> May 2006, University of Wollongong). This will provide attendees with the opportunity to network and learn about the current and potential status of information security measures, to consider their implications on citizens and business, and to identify their impact on legislation and privacy at both local and global level.
- The organization of a June 2006 workshop on Australian national C-T approaches, for 100 of Australia's leading C-T experts. This will also incorporate a research development workshop for all known PhD students undertaking a C-T related research topic.
- The 2006 RNSA conference to be held on the 21<sup>st</sup> September in Canberra will build on the success of the SET Summit, Canberra 14<sup>th</sup> July, 2005. The conference will showcase research fostered by the RNSA, with a focus on current issues in Australian CIP and comparisons with overseas experiences.
- Prof. Mike Taylor (University of South Australia), is developing a suite of four national and international workshops intended to explore transport risk and security issues. These will be held in Adelaide, Melbourne, Sydney and London later in 2006.

- The URL of the Research Network's web site.

[www.SecureAustralia.org](http://www.SecureAustralia.org)

Please note that the above information must be placed on the Research Network's web site. It must also list all sources of funding support, the Participants and their institutional affiliation, the activities supported by the Funding, and Annual Report.

The Annual Report should also report on:

All expenditure under the Approved Proposal by the Research Network, including the purchase of specific Assets or Intellectual Property; and

Funding and/or other resources provided by any other Institution, Contributing Organisation or Participant towards meeting the objectives of the Research Network.

The Financial Statement is in addition to any financial reporting included in the Annual Report.

Other information:

It would be helpful if you indicated how the Research Network:

- Has tackled or plans to tackle issues in a manner that may not otherwise have been achievable without the mechanism of a Research Network;

The RNSA is a significant vehicle in Australia today for achieving collaborative research in the area of CIP. Fundamentally, CIP research by its nature covers a wide range of disparate academic and professional disciplines. As well, the notion of CIP is not well defined as an academic or professional discipline. The presence of the RNSA has been significant in its ability to draw together a range of academic and professional disciplines not normally encountered in Australia. For instance, the merging for instance of:

- Blast modeling in engineering with human sciences to create more accurate vulnerability and threat models for buildings and built infrastructure. This work is now being merged with geographical information research as well as urban planning to develop 3-D modeling of cities, building and built infrastructure. This represents a considerable advance for emergency management as much of the current responses, and agency work are based on 2-D aerial mapping.
- C-T research into security, intelligence and vulnerability has been developed through the merging of law, criminology, science, engineering, defence and security studies, sociology, history and information systems studies.

Broadly speaking, the presence of the RNSA has been significant to achieving research collaboration in Australia, and the achieving of a national focus on the development of the academic and professional disciplines of CIP, Counter-Terrorism, Information Security and Human Factors issues in CIP. This has been achieved by the RNSA executive through playing a neutral role, organizing a program of workshops, seminars, conferences as well as attendance at university meetings giving people the opportunity to meet and exchange ideas, research interests and pool their resources.

- Has increased or is planning to increase the scale and focus of research activities; and

The RNSA has considerably increased the level of Australian research into SET (Science, Engineering and Technology) applications to CIP. For instance, increased capacity for research has been enabled through, the:

- Development of a CRC application for 2006 round of submissions (CRC-SAFE), (which is seeking funding under National Research Priority 4 –Safeguarding Australia: Priority Goal 1 – Critical Infrastructure Protection (CIP). Called CRC-SAFE), has developed several significant SET areas.
- 2005 RNSA conference/ SET Summit, held in Canberra, and the 2006 planned conference have provided a substantial opportunity for increased scale of SET/CIP research within Australia. In particular, network surveillance, CCTV applications and recognition technology, emergency management, information systems, security analysis, structures vulnerability analysis and C-T.
- November 2005 RNSA workshop on risk management and assessment for CIP brought together, academics, government, owners and operators of infrastructure and risk practitioners to capture the different views on how risk management and analysis can be improved to further the protection of Australian Infrastructure and how to build research partnerships between Industry, Government and Academia. This made important contribution to understanding the links between governance, communication and resilience in risk analysis, application and approaches.

- Has facilitated the internationalisation of research and international linkages.

The RNSA has developed a significant international profile. In 2005 the following international contacts were made:

- May/June 2005, the RNSA has formalised a research collaboration with the Imperial College, London; Centre, Royal Military College of Science, Cranfield, UK, and several UK experts in C-T. The RNSA has established a point of contact for the RNSA in UK/London through Prof David Nethercot, Head of Civil Engineering. The objectives of which was to build upon existing research and collaboration between leading Australia and UK based researchers in the area of CIP based research. The key projects under development are: transport risk and security; and building risk and security.
- The visits of several leading academics from overseas have been partly funded by RNSA funds in 2005.

Several activities to improve the international linkages have been planned for 2006.

Examples include:

- In March 2006, the RNSA funded Dr Flaherty to attend the ENEA - Italian Agency for New Technology, Energy and the Environment conference – Complex Networks and Infrastructure Protection 06, Rome. He will be representing the RNSA, and delivering a paper there at the invitation of the ENEA.
- In March 2006, Suen Yek PhD student, School of Computer & Information Science, Edith Cowan University will be attending the International Conference on Information Warfare & Security University of Maryland Eastern Shore, USA, where she will be representing the RNSA and delivering a paper. She is the first recipient of a RNSA Young Investigator Grant.

## Menu of Performance Indicators

Following discussions at the ARC Research Networks Workshop held in Canberra on 9 November 2005, we have developed the following (non-inclusive) list of possible activities on which Networks might report.

It is acknowledged that most Research Networks would not have gathered momentum until early in 2005, and that initial Annual Reports are likely to include information, to a large degree, on progress towards, rather than actual, outcomes.

Quantitative (Include, as appropriate):

Number of (active) participants:	160
Number of proposals for Network activities funded:	32
Number of ECRs funded to do various activities:	12
Number of international visits, both by Network members in Australia to overseas destinations, international events, and short and long term visits by international researchers to Australia:	6
Number of workshops, conferences or seminars conducted:	24
Number of publications produced, and their impact factors:	1 Book, Several journal articles have been submitted *More information will be collected in 2006.
Number of outreach activities including public lectures (or other forms of engagement with people outside the research community including schools, industry and government agencies):	5
Number of targeted activities: involving research interaction for postgraduate students:	3
Number of targeted activities: industry stakeholder interaction:	10
Number of universities receiving funding:	29
Number of Network web hits, articles downloaded:	3,847
Survey of Network participants to ascertain usefulness and user-friendliness of web site:	Yes
Number of opportunities for workshops to do interdisciplinary research	24
Number of national competitive grants applications and successful applications as a result of Network membership:	Several applications have been submitted

## Qualitative

Describe, as appropriate, aspects of:

- How research undertaken by the Network is different to what might have occurred without the Network;

The main impact of the RNSA on research has been the wider acceptance of multi-disciplinary approaches to CIP research. In particular:

- Better understanding of the relationship between social, legal 'implications' and the application of technology like CCTV and the impact this has on risk and security research in transport and public areas.
- The development of Centre for Policing, Intelligence and C-T (Macquarie Uni), and Centre for Counterterrorism, Security and Intelligence (ECU), both are pursuing a multi-disciplinary approach to C-T/CIP research and education. For instance, the ECU new degree - Bachelor of Counterterrorism, Security and Intelligence, is drawn together from several ECU faculties, in particular: Security Management, Computer and Network Security, Criminology and Justice Studies, Regional Security and Communication.

- Governance processes in place;

The RNSA has a Network Convenor and Administrator appointed (the University of Melbourne) work in conjunction with two other executive members (from UNSW @ ADFA, and QUT), who constitute the RNSA Management Committee. The Management Committee deals directly with the Network Participants. The members of the Management Committee are in continuous dialogue with each other, and the leader researchers among the NPs, seeking to develop collaborative research opportunities for future RNSA events. All decisions are jointly and unanimously made. The Management Committee are: A/Prof Priyan Mendis, UniMelb. (Convenor of RNSA); Prof. Joseph Lai, UNSW@ADFA (Executive Member); and Prof. Ed Dawson, QUT (Executive Member); Dr Chris Flaherty, UniMelb. (Administrator of RNSA).

The Network Convenor regularly calls a meeting with the RNSA Advisory Board. The terms of reference for the Advisory Board are that it comprises representatives of government and business who can bring an independent view on the alignment of Safeguarding Australia National Research Priorities with the work of the RNSA.

The Advisory Board provides strategic advice to the RNSA's Convenor and Management Committee on topics such as: Links with potential end-users; advice on the prioritisation of RNSA resources; advice on the relationship between the RNSA and other Australia government entities; advice on local and international developments in the CIP area; and advice on where gaps have been identified in Australia's CIP research activities.

The current membership of the Advisory Board are: Mr. Mike Rothery, Director, Critical Infrastructure Branch, Attorney-General's Dept. (Chair); Dr. Lynn Booth (Head, Prime-Minister and Cabinet, SET Unit); Dr. Tim McKenna (DSTO); Mr. Warwick Watkins (Director-General NSW Lands); A/Prof Priyan Mendis (Convenor of RNSA); Prof. Joseph Lai (UNSW@ADFA); Prof. Ed Dawson (QUT); Mr. Jason Brown (ADI Ltd.); Prof. Jannie Van Deventer (UOM, Dean of Engineering); and, Mr. Bruce Howard (Engineers Australia, Security Commissioner).

- Different kinds of research generated – research building capacity, or removing impediments to research;

The RNSA's networking activities have succeeded in developing a number of new areas of research, in particular:

- Fragmentation and Weaponisation of Buildings.
- 3D GIS Modeling (Modeling of Blast Events in Urban Environments).
- Development of Vulnerability analysis tools for building a "terrorism rating".
- Evidence v/s intelligence assessment: what are the relationship issues in law, jurisprudence and counterterrorism research.
- Evacuation planning and modeling crowd behavior.
- Identification of clustered targets, and mitigation.

- Breadth of Network - qualitative aspects;

The RNSA has developed a wide cross-section of research interests, capacities and professional capabilities. In particular, there are representative disciplines of information systems, civil and structural engineering, surveillance and security, social sciences, law, geographical information systems, economics, history, defence and security studies.

- Increased boundary crossing (multidisciplinary collaboration);

The RNSA conference and workshops have attracted participants from different disciplines. This has given excellent opportunities for networking. Broadly, researchers working on issues related to physical infrastructure security, information security and surveillance had the opportunity to explore new research areas across these boundaries. There are already ARC grant applications have been made in multidisciplinary areas.

An example of a project is given below.

#### Infrastructure Facility Vulnerability Assessment

The aim of the project is to develop an integrated low-cost multi-hazard vulnerability assessment framework/methodology applied to organizational infrastructure facilities. This framework will focus on assessing the vulnerability of organizations from a range of physical and cyber threats to the building complex, physical and cyber infrastructures. As part of this project, methodologies that assist the creation of vulnerability profiles for organizations will be developed.

This proposal brings together traditionally separated areas of research and professional expertise to address the topic of facility vulnerability assessment. These are in the areas of engineering structures, physical infrastructure security, and information technology security

- Increased or new collaboration and partnerships as a result of Network activities, and with different types of end users (e.g. industry, government and community groups);

The RNSA as has developed network relationships with the Federal and State governments. The AGs, Prime Minister and Cabinet, DSTO, CSIRO, and industry (ADI) are represented on the RNSA Advisory Board. As well, there is a close networking relationship with the Victorian, New South Wales, West Australian, Queensland and South Australian governments, and police forces. The RNSA has network members in the Defence Force, and defence industry. The RNSA has networking partners with Capital

Technic Consulting and Critical Infrastructure Protection Pty Ltd, who enable industry and government network partnering links.

- How the networks between researchers are being strengthened as a result of using web-based and other technologies;

The Network Participants are being encouraged to take an active role in the development and use of the RNSA webpage. All the network participants are given usernames and passwords. Once they enter the member area, they have access to the forum. It is expected that this forum will provide a useful platform for communication. It is also planned to launch a web based e-conference option within the website.

- Increased interest in Network, in Australia and overseas;

The RNSA has attracted a great deal of interest overseas. For example, in May/June 2005, an ongoing relationship has been created with Imperial College, London and the Centre, Royal Military College of Science, Cranfield, UK, and several UK experts in CT. The main objective of which was to build upon existing research and collaboration between leading Australia and UK based researchers in the area of CIP based research. The key projects under development are: transport risk and security; and building risk and security. The ENEA - Italian Agency for New Technology, Energy and the Environment has been interested in contact with the RNSA, seeking contributions from an Australian perspective at the conference – Complex Networks and Infrastructure Protection 06, Rome.

- What sort of additional funding was generated because of Network;

The network has not received any additional funds. However the RNSA's networking opportunities have been invaluable in the development of CIP focused research in the areas such as CCTV integration, transport security, surveillance, blast and structures which may have generated additional funding for individual groups or organisations.

The RNSA has been significant in the development of the CRC-SAFE proposal. This proposal if successful will generate an estimated \$70 million in innovative technology in the securing Australia market locally and internationally.

- How the Network has added value to the sector;

The breadth of the network allows for a full understanding of both threats and vulnerabilities relating to Australia's critical infrastructure, as well as the consideration of a wide range of risk treatment alternatives. The Network has integrated well into the existing institutional arrangements created by the Australian Government, and act as a conduit between the research community and the agencies and businesses needing assistance. The Attorney-General's Department and the Department of the Prime Minister and Cabinet are members of the Advisory Board for the Network. This ensures that the work of the Network remains in congruence with the priorities of the National Counter-Terrorist Committee and the Critical Infrastructure Advisory Council.

- What sort of different sharing /collaboration (research ideas, facilities etc) arose because of the Network;

Several discussions have been held among researchers on sharing of resources. It is expected that some useful collaborations will emerge during this year as a result of the activities commenced in 2005.

- What successes, if any, have occurred during the reporting period;

The launch of the network by the Attorney-general at the Parliament House in Canberra attracted considerable media attention. Many senior government officials and industry leaders attended the launch.

Researchers had the opportunity to meet government and industry representatives working in areas related to CIP during the SET Summit in July 2005. One of the highlights was the plenary session involving the presentations from members of PACT, Dr Greg Simpson, Coordinator of the Secure Australia Program, CSIRO, Neil Bryans, Director Information Sciences Laboratory, DSTO, Dr Ron Hutchings, Coordinator National Interest and Capability Enhancement, ANSTO, and Dr Phil McFadden, Chief Scientist, Geoscience Australia. The Hon Gary Nairn MP, Parliamentary Secretary to the Prime Minister, Dr Lynn Booth, Department of Prime Minister & Cabinet and Mr. Mike Rothery, Attorney-General's Department also attended the plenary session.

What disappointments, if any, occurred during the reporting period;

None

- How new skills have been acquired as a result of research technology;

The outcomes from the initiatives introduced in 2005, will be known in the next few years.

Examples:

The formation of the network helped to organise a special industry/academic group to be involved in explosion testing in Woomera. This will help to develop several high quality research projects.

- Any surveys carried out of members to ascertain any benefits gained from membership of the Network;

The RNSA Administrator has held numerous dialogues with the Network Participants (NPs) seeking feed back on the development of the RNSA. This also includes email contacts to current NPs. A survey will be conducted this year.

- Outreach activities and how these may have been reported by the media;

The main communications tools for the RNSA's outreach contact (and media) are the RNSA webpage ([www.secureaustralia.org](http://www.secureaustralia.org)) and the use of Australian Homeland Security Research Centre (AHSRC), and Critical Infrastructure Protection Pty Ltd. (which is currently developing the CRC-SAFE application) to develop and enable industry contact with the RNSA. The RNSA Administrator (Dr Flaherty) also regularly provides events-reports for the AG's Dept. CIP Newsletter (<http://www.tisn.gov.au>). As well, the AHSRC maintains both a webpage ([www.homelandsecurity.org.au](http://www.homelandsecurity.org.au)) a data-base and email list of Australia's homeland security professionals, which is also distributed to media outlets. This carries RNSA updates and news. Additionally, over the previous several months there have been a number of media releases profiling the RNSA. In particular:

- "Research forum planned for infrastructure security", Australian Financial Review, 21/02/05
- "Steady progress towards a broader strategy document - National Security", The Australian, 25/02/05

- Network to Research Protection, Australian Financial Review, 21/02/05
- "Terrorism: Australia launches research body", ANSA - English Media Service, 24/02/05
- "Fed: Anti-terror researchers join forces", Australian Associated Press General News, 23/02/05
- "Experts join war on terror", Melbourne MX (evening paper), 23/02/05
- "Anti-terror force", Northern Territory News/Sunday Territorian, 23/02/05
- Melbourne welcomes the launch of "Secure Australia" research network. UniMelb Media Release (Thursday 24 February 2005).  
[http://uninews.unimelb.edu.au/articleid\\_2101.html](http://uninews.unimelb.edu.au/articleid_2101.html)
- HSC Net ARC Research Networks. [www.hcsnet.edu.au/arcnetworks](http://www.hcsnet.edu.au/arcnetworks)
- 2m for Research to Safeguard Nation's Critical Infrastructure. UniNews Vol. 13, No. 21 (15 - 29 November 2004). [http://uninews.unimelb.edu.au/articleid\\_1921.html](http://uninews.unimelb.edu.au/articleid_1921.html)
- Australian Research Network in Security. ERCIM News No. 63 (October 2005). [http://www.ercim.org/publication/Ercim\\_News/enw63/dawson.html](http://www.ercim.org/publication/Ercim_News/enw63/dawson.html)
- Network To Research Protection. <http://www.webprowire.com/summaries/983602.html>
- Melbourne Welcomes the Launch of "Secure Australia" Research Network, Defence and Homeland Security, Weeks - FEB 14 - 28, 2005.  
[http://www.urwatch.com/defense%20&%20homeland%20security\\_files/defense-feb01-28--05.htm](http://www.urwatch.com/defense%20&%20homeland%20security_files/defense-feb01-28--05.htm)

- Collaborations between Networks in Australia;

It is planned to organise a joint workshop on "Complex Systems Approaches to Critical Infrastructure" with Complex Open Systems Network and Sensor systems network. A joint workshop on SCADA systems is also planned with the Sensor systems network.

- Linkages with international Research Networks; and

RNSA is the only research network dealing with CIP. Although there are no formal international networks, the funding will help the individual researchers to strengthen links with world leaders in research areas related to CIP.

- Development of tools, software, databases.

- Development of RNSA webpage.
- Development of electronic database of Network Participant members, academic profiles, and contact information using PHP and MySQL.
- Development of CIP Directory of Safeguarding Australia Capability, listing RNSA Industry Partners and Commonwealth & State Agencies (which is linked to the Australian Homeland Security Research Centre directory at - <http://www.homelandsecurity.org.au/Directory.htm>)

Financial Statement

ARC Research Network name: Research Network for a Secure Australia

Administering Organisation: The University of Melbourne

Sources of Funding: **(Aug. 2004 – Dec. 2005)**

• ARC Network Grant	\$593,150.00
• Contributing Organisations (cash and in-kind)	\$600,000.00
TOTAL:	\$1193,150.00

Expenditure of the ARC Research Network Grant Funds:

(Please report on the expenditure on the items as stated in the Approved Proposal for the Research Network)

## • Personnel Salaries and on-costs, such as:

The Network Convenor	\$00.00
Research Associates, professional officers, technicians, laboratory attendants, administrators, organizers	\$41,245.03
Specialist professional staff located within major facilities and other appropriate settings	\$83,280.02.

## • Shared Research Resources, such as:

Social Surveys	\$00.00
Software tools	\$20,800.21
Databases	\$00.00

## • Bringing People Together, such as:

Workshops	
Meetings	
Seminars	
Conferences	
Total for above items	\$41,267.23
Planning, co-ordination activities	\$2,977.76
Travel	
Accommodation	
Total for above items	\$99,139.08
Purchase of specific Assets or Intellectual Property	\$00.00

## Other expenditure:

Any other expenditure not falling under the specified expenditure headings above	\$00.00
TOTAL EXPENDITURE	\$288,709.33
Carryover amount:	\$ 304,480.67

- The funds were available only in March 2005, therefore temporarily some other accounts were used. \$48,922 to be transferred to a different account.. (\$40000 for Network Convenor and \$8922 for Network Administrator). Therefore actual carry over is \$255,558.67.

Provide the reason for carryover in the column below:

Although some activities continued from the seed funding stage, that network was officially launched in Feb. 2005. Therefore half-year funding (2004) should be carried over. Some savings were also made by combining the RNSA conference with the Safeguarding Australia conference (in Canberra). Extensive use of venue facilities within the Universities (e.g. ADFA) helped to reduce the costs of workshops. These extra funds will be utilized for other activities (workshop planning for research leaders) during this year.

It is essential that reasons be provided by carryover requests

It is the responsibility of the Research Network to ensure that the carryover amount requested in this document is the same as that which is forwarded electronically to the ARC by their Institution's Administration in a separate End of Year Report.

Research Network Convenor or Delegate:

A/Prof. Priyan Mendis (Research Network Convenor)

---



Signature: \_\_\_\_\_

Date: 31/03/2006