

Administered by



Research Network for a  
Secure Australia  
Protecting Australian Infrastructure

Funded by



Australian Government  
Australian Research Council

## RESEARCH NETWORK FOR A SECURE AUSTRALIA RNSA

### ANNUAL REPORTING REQUIREMENT TO ARC

#### **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 for 1/01/07 to 31/12/07:**

*Attachment 1* describes reporting requirements that are based on the Research Networks Funding Agreement.

*Attachment 2* 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.

*Attachment 4* is a list of RNSA members as at 29 February 2008.

## Attachment 1

### 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 since the commencement of the RNSA in 2004/2005 (The network was officially launched in 2005 Feb.). 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, in past few years, has been successful in achieving its networking goal in bringing together Australia's leading researchers, government and industry leaders involved in 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 since 2004/2005, 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 Science and Security Division (NSST Unit) and Emergency Management Australia (EMA).

The advisory board of RNSA consists of representatives of these organizations and industry.

The present Advisory Board consists of:

- Mike Rothery-Chair (Director, Critical Infrastructure Branch, Attorney-General's Dept.).

Members:

1. Dr. Richard Davis (Head, Dept. of Prime-Minister & Cabinet, NSST Unit);
2. Dr. Lynn Booth (DSTO);
3. Mr. Bruce Howard (Engineers Australia, Security Commissioner);
4. Prof. Ed Dawson (QUT);
5. Prof. Peter Anderson (PICT, Macquarie University);
6. Mr. Jason Brown (General Manager, Thales);
7. Craig Sharkie (CSL Ltd);
8. Tony Sleigh (NSW Lands);
9. Mr. Warwick Watkins (Director-General NSW Lands);
10. Prof. Priyan Mendis (Convenor of RNSA);
11. Prof. Joseph Lai (ADFA);
12. Ms. Jennie Clothier (DSTO);
13. Mr. Terry Vincent (Australian Bomb Data Centre).
14. Prof. Hussein Abbass (ADFA)

Advisory Board Secretary:

- Mr. Athol Yates

**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 407 (a further increase of 27% from 2006) 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 as follows:

These events contributed to the RNSA mission statement of facilitating 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. A number of excellent contacts were made between the participants and speakers.

#### Significant Workshops and conferences

##### 1. USA-TSWG/RNSA workshop -14<sup>th</sup> March 2007

The USA-TSWG (<http://www.tswg.gov/>). is the main US agency funding and co-ordinating security related research. RNSA organized a workshop/focus group meeting to present academic and industry research in Australia. 87 participants from Government Departments, Industry and Academics attended the forum at ADFA. Speakers from Australia were followed by moderated panel with US subject matter specialist and discussion The meeting was partly sponsored by the Dept. of Prime-Minister & Cabinet, NSST Unit.

The presenters were

Session 1: Explosive Detection, Forensics

- Chris Lennard (University of Canberra)

Session 2: Blast Effects and Mitigation

- Priyan Mendis -Overview of Australian Research and development
- Mark Rebentrost (VSL Ltd)- Advanced Materials for blast protection
- Nigel Buckley (AV S-elli Ltd.)- Development of a Blast Barrier

Session 3: CBRN

- Steve Wilkinson (Chemistry Centre WA)

Session 4: Infrastructure Protection

- Andrew Clark (QUT) Cyber Security, overview
- Kevin Foster (Connell Wagner) Physical Security

Session 5: Surveillance

- Hussein Abbas (ADFA)- Analytic Surveillance, Information operations support
- Brian Lovell (UQ)-CCTV and other traditional surveillance
- Rustom Kanga (iOmniscient) -Intelligent Surveillance

2. The Inaugural RNSA Terrorism History Conference “Lessons of the Past: Applications of History for Today's Threats” on 14 June, 2007 at International Affairs Conference Centre, Canberra hosting participants from defence, academic, industry and policing backgrounds.

The details of the presentations are given below:

1. Transdisciplinarity, signature pedagogy and the place of History in Terrorism Studies - Dr Sean Brawley, Senior Lecturer, School of History, UNSW
2. Terrorism Studies: The Dismal Science? - Prof. Carl Thayer (UNSW@ADFA)
3. The application of history to Terrorism Studies: The reflections of a practitioner/scholar - Prof. Clive Williams (ANU)
4. The Use of History by Lawyers in Debating Responses to Terrorism - Dr. Andrew Lynch (UNSW)
5. The lessons of the Irish Experience - Prof. Mark Finnane (Griffith)
6. The lessons from anarchists/nihilists and co-travellers of the late 19th century and early 20th centuries - Don Williams

## 7. Intelligence Pathologies in Terrorism Analysis - Brett Pepler

### 3. RNSA Security Technology Conference on 28 Sept 2007 in Melbourne

119 academics, researchers and industry members attended the conference. There were 38 presentations in 4 parallel streams. The conference has become an annual event bringing together both researchers and practitioners in the fields relating to the national research priority area of Safeguarding Australia. It provided a forum for the exchange of ideas and research findings between core groups and individuals interested in security technology.

The opening address was given by The Hon. Phillip Ruddock, Attorney-General. The title of the speech was "The role of academics and industry in developing products and services for national security". Welcome speech was given by the Vice-Chancellor of the University of Melbourne, Prof. Glyn Davis. The plenary speakers were Professor Rob Evans on Recent developments in security applications-Wireless sensor networks; Mr. Mike Rothery, Chairman of the RNSA Advisory Committee and Assistant Secretary of Critical Infrastructure Protection Branch on The research and development needs of the critical infrastructure sector; and Mr. Paul Murphy from GHD on Lessons from the lab to deployment for security technology.

A 397-page book titled "Recent Advances in Security Technology" consisting of all the refereed papers from the conference was produced. Each paper was subjected to a rigorous review process conducted by at least two experts in the appropriate field.

4 Workshops were held addressing these questions:

1. What are the key trends in this area?
2. What are the reasons for stopping the technology from being implemented faster?

Workshop 1 - Decision support tools for incident management

Workshop 2 - Blast modelling and analysis

Workshop 3 - Smart surveillance

Workshop 4 - Social science (related to CIP)

### 4. A workshop on Anticipating Climate Change risks, costs and opportunities for infrastructure in Melbourne on 21 June 2007.

The attendees consisted of 13 speakers and 60 delegates

As there is more than \$800 billion of infrastructure assets in Australia with over \$30 million currently being planned, the threat that climate change poses to these assets requires careful impact analysis and mitigation strategies. This event which is Australia's first in-depth symposium on identifying the effect of climate change on infrastructure was supported by:

\* Australian Academy of Technological Sciences and Engineering

(ATSE) and

\* Institution of Engineers Australia

This symposium was designed to

- \* identify the climate change risks in a rigorous way
- \* plan for the probable changes
- \* identify upside risk of climate change
- \* understand the looming pressures from different groups on infrastructure owners

The presentations were given by

1. "The big picture with climate change and infrastructure"

Dr John Marsden, Marsden Jacob Associates, contributing author of the Greenhouse Office's Climate Change Impacts & Risk Management - A Guide for Business and Government

2. "Risk - What is it?"

Whole of infrastructure business risks; Valuing and comparing risks; The comparative rise in importance of climate risk; Greenhouse gas generation and infrastructure projects

Roger Byrne, International Manager - GHD Asset Management Group

3. Identifying the impacts of climate change on infrastructure

Identification of likely climatic changes relevant to infrastructure planning, such as: increased temperatures; increased sea level; changes to rainfall and water availability

Paul Holper, CSIRO Manager of the Australian Climate Change Science Program and co-author of Infrastructure and Climate Change: Risk Assessment for Victoria (May 2007), the first Australian study examining the potential risks to a range of infrastructure types.

4. "Assessing climate change risks – A finance sector perspective"

Physical and regulatory risks, Dealing with regulatory uncertainty, Differences in markets, eg European versus Australia, The need for climate change risk disclosure - Expectations in Australia and internationally

Dr Ian Woods, Sustainable Alpha Funds Team, AMP Capital Investors.

5. "Applying 4360 to managing the risks of climate change"

Climate change risk management framework, Conducting an assessment, Addressing uncertainty and sensitivity, Integration with existing risk management practices

Peter Kinrade, Marsden Jacob Associates, contributing author of the Greenhouse Office's Climate Change Impacts & Risk Management - A Guide for Business and Government

6. "Assessments of impacts of climate change on Australia's physical infrastructure"

Prof. Len Stevens, Department of Civil and Environmental Engineering, University of Melbourne

7. "Climate Change and Infrastructure"

Michael Nolan, Principal Consultant - Sustainability, Maunsell Australia and co-author Infrastructure and Climate Change Risk Assessment for Victoria (May 2007).

8. "Developments in contracts, compensation and development approvals"

Contract clauses and variations due to climate change, Compensation for loss of value due to climate change, Changes in development approvals due to climate change Implications for investors, councils and the community

Louise Hicks, Partner, DLA Phillips Fox

#### 9. "Business in a (Climate) Changing World "

The evolving need for new products under climate change, Leveraging assets and infrastructure for commercial opportunity, Impacts of climate change on property markets, Impacts of climate change on insurance

Dr Karl Mallon, Scientific and Technical Director, Climate Risk Pty Ltd. Climate Risk provides specialist climate change risk analysis for government and the private sector.

#### 10. Panel on the demand for climate change risks to be factored into infrastructure decisions

The panel addressed the question "What groups will contribute to pressure for climate change to be factored into infrastructure decisions, and how will they apply it?"

##### Panel Members

- Kenneth Davidson, Business Staff Columnist, The Age, and Co-Editor, DISSENT
- Adjunct Professor David Hood, Department Built Environment & Engineering, Queensland University of Technology
- Ivan Donaldson, Executive Director, Australian Building Codes Board
- Dr Don Fry AO, Chairman AIMTEK and representative of Society for Sustainability and Environmental Engineering

**5. Workshop on Network Monitoring: Identifying and Measuring the Threat** on 4 September, 2007 at the Crown Plaza Surfers Paradise Hotel, Gold Coast attended by 31 participants including academics, researchers, research students and government and industry people. The presentations provided broad coverage of the many different facets of network monitoring focusing on challenges and leading edge activities in the area of network threat monitoring.

The workshop featured several distinguished presenters from Europe, North America, and Australia. The details of the presentations are given below

1. Opening Address: Ed Dawson (QUT)
2. Network Monitoring – Operational Challenges: Graham Ingram (AusCERT, Australia)
3. Host and Subnet Behaviours: Visualization for Measurement and Insight: John McHugh (Dalhousie University, Canada)
4. Leurré.com V2.0: Beyond Low Interaction Honeypots: Marc Dacier (Institute Eurécom, France)
5. Analyzing Malicious Code: Christopher Kruegel (Technical University Vienna, Austria)
6. Monitoring a Network Service without Knowing the Threat: Ludovic Mé (Supélec, France)
7. Cybersecurity and Critical Information Infrastructure Protection: Olivier De Vel (DSTO, Australia)
8. True Challenges of 21<sup>st</sup> Century Information Security R&D: Ming-Yuh Huang (The Boeing Company, USA)

6. ICE-EM RNSA 2007 Workshop on 27-29 June, 2007 at Queensland University of Technology, Gardens Point Campus, Brisbane attended by 46 participants including academics, researchers, overseas delegates and industry people. The main aim of this workshop was to discussions led by experts on the latest issues impairing cryptography (relevant to Australia).

Keynote lectures were presented by Prof. Kenny Paterson, Royal Holloway, London, Dr.Xavier Boyen, Voltage Security Inc, USA, Dr. Andreas Enge, Ecole Polytechnique, France, Dr. Michael Scott and Prof. Willy Susilo, University of Wollongong, Australia.

7. Second Workshop on Social Implications of National Security: From Dataveillance to Ubeveillance on 29 October, 2007 at the University of Wollongong

The Workshop was organised by RNSA members from the IP Location-Based Services Research Program (Faculty of Informatics) from the University of Wollongong. It provided a forum for the exchange of ideas and research findings between core groups or individuals interested in the social implications of national security measures, focused on the big picture question of Surveillance vs Security.

Workshop participants learnt about the current and potential status of information security measures. The notion of Dataveillance and that of Ubeveillance were contrasted in the context of national security. What is the price of security that citizens are prepared to pay? Will surveillance technology force us to choose between our right to privacy and national security? This workshop delved deeper into some of the pressing issues facing technology innovation and adoption, government policy, and the legal and regulatory framework.

The cross-disciplinary workshop was seeking perspectives which covered a diverse array of interest areas such as security, information technology, law, philosophy, sociology, religion, politics, history, culture, science and technology studies, and business.

The workshop included papers by Associate Professor of Counter-Terrorism Nicholas O'Brien, Professor of Social Sciences Brian Martin, Professeur des Universites Invité Université d'Orleans George Mickhail, Associate Professor of Law Gregory Rose and Professor of Transport Systems Marcus Wigan.

Other presenters included Professor Roger Clarke Principal of Xamax Consultancy (keynote), Mr Rob Nicholls and Ms Michelle Rowland lawyers and Dr Lucy Resnyansky a research scientist with the DSTO, and the QUT, Information Security Institute's Dr Lauren May.

Other key seminars/workshops/conferences organized include:

- 3rd Indo-Australian Conference on Information Technology Security (IACITS) 2007 on 9-10 July, 2007 at the Queensland University of Technology
- 12th Australasian Conference on Information Security and Privacy (ACISP) 2007 on 2 - 4 July, 2007 at Townsville, Queensland.
- International Conference on Provable Security (ProvSec) 2007 on 31 Oct–2 Nov 2007 at Wollongong, NSW
- 8th Australian Information Warfare and Security Conference 2007 on 3–4 December,

2007 at Edith Cowan University, WA, Australia.

- Australian Earthquake Engineering Society Conference 2007 on 23-25 November 2007 at Wollongong, NSW.

RNSA Sponsored visits to two Universities in US for Jason Smith, Research Fellow, Information Security Institute, Queensland University of Technology on 20 – 30 April 2007 with extensive information security and critical infrastructure protection programmes.

In addition to the sponsorship of several keynote speakers for conferences mentioned above Sponsorship of overseas researchers from various universities and institutions as follows:

- Andreas Enge from France - invited speaker and presenter of 8th International Conference on Finite Fields and Applications on July 9-13, 2007 in Melbourne Australia
- Prof. Andrew Whittaker from University of Buffalo - An expert on design of nuclear structures, also an expert on seismic design and blast design of structures

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

Several key achievements of the RNSA, in particular are:

Several important international links were established during 2007 with USA, Europe, Canada, China, Singapore and India. The links were developed by events sponsored by RNSA such as organizing joint workshops, Australian academics (sponsored by RNSA) attending international conferences, special meetings organised by the network convener and Advisory board members making presentations on behalf of RNSA during overseas visits.

The continued support in 2007 (as for 2006) from the Attorney-General and his department 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 and industry.

Two significant documents on directories of Australian research related to transport security and the CBRN (Chemical, Biological, Radiological, Nuclear) sector were prepared by RNSA (partly sponsored by Dept. of Prime-Minister and Cabinet, NSST unit) for PACCT group (Public Agencies Collaboration for Counter-Terrorism).

A study conducted (commenced in 2006) by the Academy of Technological Sciences and Engineering to assess the effect of climate change on natural hazards and the resultant impact on the risks to major infrastructure was partly sponsored by the Research Network (RNSA).

RNSA participated in the development of a CRC application (CRC-SAFE) for the last round of submissions, seeking funding under National Research Priority 4 -Safeguarding Australia: Priority Goal 1 -Critical Infrastructure Protection (CIP). This application was supported by a broad based consortium of university, government and industry. This activity significantly mobilised Australian CIP research and industry support and engagement with this research.

The application reached the last round, but was unsuccessful. However the established links helped to develop a number of industry supported applications such as the ARC linkage.

The RNSA also helped to bring together some researchers for the applications for ARC's Centre of Excellence for Security and Policing. RNSA will be involved in the newly formed ARC COE at Griffith University.

As for previous year, RNSA spent time in 2007 planning for the following to occur in 2008:

Improved International Collaboration (TSWG, EU, Singapore etc.)

Interaction with Govt. Agencies (PACCT, EMA etc.)

Several events have been planned for 2008. Some examples are given below.

Name	Date/Venue
The 3rd International Conference on Design and Analysis of Protective Structures & Assets (DAPS) 2008	November 10-12 2008/ Melbourne
ACISP'2008 conference	July 7-9.Wollongong
ASIACRYPT'2008 conference This is to be held in	December 7-11 Melbourne
Mass transport conference	November Brisbane
Third Workshop on Social Implications of National Security:	October at the University of Wollongong
Smart Decision Making for Clean Skies (Modern Air Traffic Management and the Environment)	July in Canberra
Operations Research in Australia: The Experts Speak!	July in Canberra

The KPI's for RNSA 2008 are consistent with the ARC measures set out in Annual Reports and include such things as:

- Increase in active member participants by at least 15%
- Increase in number of article published by 25%
- Increase in the number of articles, presentation and resources from workshops, conferences etc on the RNSA website by 100%
- Increase in number of website hits
- Maintain the number of workshops/conferences/research conducted and attract more early career and post grad researchers
- Maintain governance effectiveness by maintaining meetings, reporting and key financial reports
- Improve mechanisms for communications amongst network members, via the secure website, newsletter or otherwise

## Key Strategies

Some on-going activities and critical strategies which will be pursued in the next 12-18 months are as follows:

1. Identify 6 academic/industry champions in key areas and support them in developing collaborative activities including conferences, workshops and reports
2. Provide opportunities for researchers and industry to promote their research and developments via workshops and courses
3. Provide opportunities for the user community to identify relevant researchers and developments by developing a publicly searchable online database of Australian researchers which include RNSA and non-RNSA members
4. Provide opportunities specifically aimed at building teams to win research grants, and industry-government-university projects

## Attachment 2

### Menu of Performance Indicators

A comparison of the performance of 2005 (effectively 1.5 years) and 2006 (one year) against 2007 (one year) and 2008 (target) is given below.

TYPE OF MEASURE	2005	2006	2007	2008 (target)
Number of (active) participants:	160	292	407	>500
Number of proposals for Network activities funded:	32	40	40	30-40
Number of ECRs funded to do various activities:	12	18	40	>40
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	6	8	8
Number of workshops, conferences or seminars conducted:	24	16	16	>15
Number of publications produced, and their impact factors:	1 Book	2 Books	2 Books See note 1	>2
Number of outreach activities including public lectures (or other forms of	5	5	6	>5

RNSA Annual Report, 2007-2008

engagement with people outside the research forms community including schools, industry and government agencies):				
Number of targeted activities: involving research interaction for postgraduate students:	3	3	5	>5
Number of targeted activities: industry stakeholder interaction:	10	15	15	>15
Number of universities receiving funding:	29	22	24	>24
Number of Network web hits, articles downloaded:	3,847	10,707	14,000	>18,000
Survey of Network participants to ascertain usefulness and user-friendliness of web site:	Yes	Yes	Yes	Yes
Number of opportunities for workshops to do interdisciplinary research	Difficult to Quantify	Difficult to Quantify	Difficult to Quantify	
Number of national competitive grants applications and successful applications as a result of Network membership	Several submitted	Several submitted -Difficult to quantify	Several submitted - Difficult to quantify	

Note 1 – RNSA has published two books in 2007. One book published in conjunction with RNSA’s annual Security Conference and the other book related to the Second Workshop on Social Implications of National Security: From Dataveillance to Uberveillance.

## 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 since 2004/2005 has been the wider acceptance of multidisciplinary approaches to CIP research and the industry uptake. Already RNSA has helped several researchers to collaborate in multi-disciplinary research. The presentations during TSWG meeting in March 2007 and RNSA conference in 2007 highlighted this type of research. The comments by the US-TSWG Group Chair confirms this observation. (US-TSWG is the main US agency funding and co-ordinating security related research.)

RNSA also helped to develop links for some ARC linkage infrastructure applications. Some of the activities and networking forums have helped to avoid unnecessary duplication of research. Also these forums have helped to identify new research themes and sub themes related to CIP.

### Governance processes in place;

The RNSA normally, has a Network Convenor and Administrator appointed (the University of Melbourne). The Network Administrator resigned with short notice. Alternate arrangements were made to continue the various activities of the network. Some of the administration activities were transferred to outreach manager (Athol Yates and his office in Canberra). This arrangement worked very effectively. The network convenor continue to work in conjunction with three other executive members (from UNSW @ ADFA, and QUT), who constitute the RNSA Management Committee. Prof, Hussein Abbass, Professor and Chair of Information Technology at UNSW at ADFA and Director of the Defence and Security Applications Research Centre (DSARC) joined the management committee in 2007, The Management Committee deals directly with the Network Participants. The members of the Management Committee are in continuous dialogue with each other (through face to face meetings and regular teleconferences), and the leading researchers among the NPs, seeking to develop collaborative research opportunities for future RNSA events. All decisions are jointly and unanimously made. The Management Committee members are: Prof Priyan Mendis, UniMelb. (Convenor of RNSA); Prof. Joseph Lai, UNSW@ADFA (Executive Member); Prof. Ed Dawson, QUT (Executive Member) and Prof. Hussein Abbass. .

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 is given in Page 2. It was decided to increase the industry representation in the board. Craig Sharkie from CSL Ltd. was invited to join the

Advisory Board in 2007;

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 (as presented in previous reports), in particular:

- Intelligent Building Airflow Systems Configuration, Detection and Response
- Social and Individual Issues in Terrorism and Criminality
- Plume & Dispersion Modeling for CBRN
- Smart Evacuation, Egress and Emergency Response
- Air Toxin Reduction via Scrubbing and Chemical Destruction/Neutralization
- Biometrix/Biomedical in Emergency Response Training and Evacuation
- Mobile/Wireless Device Security Systems
- Object Continuity Across Hetrogenous Distributed Sensor Networks (Object Tracking)
- Framework and Decision Support in Hetrogenous Networks and Applications to IED Detection
- Advanced SCADA Security Systems
- Low Cost Sensors for Toxic Materials
- 3D GIS Modeling (Modeling of Blast Events in Urban Environments)
- Development of Vulnerability analysis tools for building a "terrorism rating"
- Evidence via 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.

Several papers relating to these areas have been presented in RNSA annual conference.

Breadth of Network - qualitative aspects;

The RNSA has 3 major areas and nodes (as presented in the main application); Physical Security, Information Security and Surveillance & Intelligent Systems. These broad areas include several disciplines such as information systems and security, electrical engineering, computer science, geomatics, civil and structural engineering, surveillance and security, social sciences, law, geographical information systems, economics, history, defence and security studies. Academics from Medical faculties (e.g. University of Newcastle) have also joined the network.

Increased boundary crossing (multidisciplinary collaboration):

The RNSA has developed a wide cross-section of research interests, capacities and professional capabilities as mentioned in the previous section. The RNSA conferences and workshops held in 2005, 2006 and 2007 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. These relationships have led to many ARC grant applications in multidisciplinary areas. However it is difficult to quantify them.

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):

As mentioned in previous sections, RNSA is the leading forum in Australia bringing together Australia's leading researchers, government and industry leaders involved in Critical Infrastructure Protection (CIP). The RNSA has developed network relationships with the Federal and State governments and the industry. The AGs, Prime Minister and Cabinet, DSTO, EMA, Engineers Australia and industry (ADI and CSL) are represented on the RNSA Advisory Board. The RNSA also has a close relationship with Trusted Information Sharing Network (TISN) developed by the CIP branch of the Attorney-General's Dept. which includes industry stake holders. Representatives from community organizations such as Salvation Army have attended RNSA forums.

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

A website tracker has confirmed that the RNSA website (<http://www.secureaustralia.org>) attracts visitors from Australia and overseas. Only NPs (Network participants) get access to the protected area of the website. All the registered NPs are given usernames and passwords. Once they enter the member area, they have access to the secure forum. The forum provides a useful platform for communication. Further, participants are able to access workshop papers and summaries from this secure workshop including:

- papers and summary overheads presented at the CT Workshop
- Papers (PDF files) from the 2005,2006, 2007 conferences
- Podcasts of selected presentations from some RNSA forums

Increased interest in Network, in Australia and overseas:

The RNSA continues to attract a great deal of interest overseas. During the last TSWG meeting in March 2007, the leader of the TSWG delegation recognized the important contribution of the network (RNSA) to the CIP and in general the security community. He also mentioned that similar networks do not exist in USA. Similar comments have been received from international leaders (in CIP) that this organization is unique in the area of CIP and that many European contacts will be seeking to replicate the mission and function of RNSA in their countries.

What sort of additional funding was generated because of Network;

Although difficult to quantify, many researchers have received additional funding from different sources due to the contacts developed through the involvement in the RNSA activities. RNSA's networking opportunities have been invaluable in the development of CIP focused research in a number of 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. Although this proposal was not successful this round, discussions are underway to reapply in the next round. The links developed through this application will lead to grant applications in other schemes such as ARC linkage.

How the Network has added value to the sector;

As mentioned in the previous reports, 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, Department of the Prime Minister and Cabinet, Emergency Management of Australia 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 and various IAAG's (Infrastructure Advisory Assurance Groups)

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. Already these collaborations have led to the development of common facilities (e.g. High Rate Testing System for Materials and Structures initiated by Swinburne University). The RNSA also facilitated the involvement of Australian researchers and industry participants in the Woomera blast trials. It is expected that some useful collaborations will emerge during this year as a result of the activities commenced in 2005, in 2006 and in 2007.

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

Researchers had the opportunity to meet government and industry representatives working in areas related to CIP during the Annual Conference in September 2007 and other forum organized by the network.

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

The RNSA has been successful in getting many academics involved with the network. Many

ECRs have also joined the network. It is very difficult to get feedback from some NPs about the successes achieved through the involvement in the network.

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

The outcomes from the initiatives introduced from 2005 to 2007, will be known in the next few years. The latest developments were presented in the TSWG forum in Canberra (as mentioned in Page 4)

There are other examples such as the network helping to organise a special industry/academic group to be involved in explosion testing in Woomera in 2006 and 2007. 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 outreach manager 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.

NP's have welcomed the opportunities to be able to use RNSA secure website to exchange ideas and network in a secure environment.

The following SWOT analysis was prepared with the feedback received from the NPs.

***Strengths, Weaknesses, Threats & Opportunities***

**Strengths:**

- Comprehensive academic membership
- Strong advisory board
- Strong management team
- Good links with major security agencies

**Weaknesses:**

- Over-emphasis on counter-terrorism
- Lack of motivation for members to initiate action as no research income automatically comes
- Overdependence on few key staff
- Limited benefit of node structure
- Low industry involvement

**Opportunities:**

- Broaden focus from CIP to any organisation with a security interest
- Broaden to cover all-hazards
- Broaden to include social science
- Deliver on developing links which bring research dollars
- Delivery on developing industry-government-researchers collaboration
- Engage the enthusiasm of champions to lead collaborative activities
- Increase multi-disciplinary activities

**Threats:**

- Funding ends in 2008/2009.
- Alternative mechanisms appear to bring together researchers, industry and community
- Lack of interest in multi-disciplinary research-CIP (Researchers).

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) to develop and enable industry contact with the RNSA. The RNSA Administrator also regularly provides event reports for the AG's Dept. CIP Newsletter (<http://www.tisn.gov.au>). As well, the AHSRC maintains 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.

Some Individual members of RNSA have appeared in radio and television interviews and newspaper articles related to CIP. For example the cover story of the Channel 9, Sunday program in Sept 2007 was about the protection of infrastructure in Australia. Some network members including the convener appeared in the program.

Collaborations between Networks in Australia:

Regular contacts with the other networks have been maintained through e-mail. Discussions have been held with other networks such as the sensor systems to organise joint activities. A joint workshop is planned with sensor systems network to organise a forum on ICT for Sustainability, in 2008.

Linkages with international Research Networks; and

As mentioned in previous sections, the RNSA is the only research network in the world 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..

As mentioned in previous reports, the RNSA has completed the following:

- 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>)
- Assistance in preparation of the transport security expert directory.
- Databases (Research Projects and Researchers in Australia) for Transport Security and CBRN research.
- CIP Directory for Researchers (under preparation)

## Attachment 3

### Financial Statement

ARC Research Network Name: Research Network for Secure Australia (RNSA)

Administering Organisation: The University of Melbourne

Jan 07 to Dec 07

#### Funding Details:

##### Sources of Funding

	Amount	
	Cash	In-kind
ARC Network Grant for 2007	\$413,972.00	
ARC Network Grant Carried forward from 2006	\$155,753.22	
Contributing Organisations (cash and in-kind contributions by each organisation)	\$175,209.27	\$560,000.00
<b>Total Available Funding</b>	<b>\$744,934.49</b>	<b>\$560,000.00</b>

List of Expenditures Description	2007 ARC Research Network Funding Amount	Contributing Organisation contributions	
		Cash	in-kind
<b>Personal Salaries and On-costs</b>			
Network Convenor		\$107,855.00	\$150,000.00
Research Associates, Professional Officers, Technicians, Laboratory Attendants, Administrations and Organisers	\$45,485.82		
Specialist Professional Staff Located with Major Facilities and Other Appropriate Settings	\$117,916.29		
<b>Shared Research Resources</b>			
Social Survey			\$10,000.00
Software Tools			
Databases	\$20,000.00		\$240,000.00
Trial Instrumentation and Equipment Charges	\$18,066.63		
<b>Bringing People Together</b>		\$377.00	
Workshops	\$15,337.80		
Meetings	\$12,143.36		
Seminars	\$5,359.97		
<b>Conferences</b>		\$43,692.00	\$20,000.00
Travel	\$29,651.14		\$100,000.00
Other	\$27,609.07		
<b>Planning, Coordination Activities</b>			
Travel & Accommodation	\$77,690.74		
Purchase of Specific Assets or Intellectual Properties	\$1,590.00		
<b>Other Expenditures</b>		\$23,285.27	\$40,000.00
Not Falling Under the Specified Expenditure Heading Above	\$28,451.91		
<b>Total Expenditure</b>	<b>\$399,302.73</b>	<b>\$175,209.27</b>	<b>\$560,000.00</b>
Carry Over Amount (As at December 2007)	\$170,422.49		

Provide the reason for carryover in the column below:

The network was officially launched in Feb. 2005 (the funding commenced in mid 2004). Therefore an amount close to half-year funding (2004) should be carried over. So a carry over figure appears. Some invoices (about \$40000) were paid after December 31<sup>st</sup> for activities conducted in 2007. Therefore the actual carry over should be smaller than the reported carry over figure.



Research Network Convenor or Delegate:  
Prof. Priyan Mendis (Research Network Convenor)

## Attachment 4

A list of RNSA members as at 29 February 2008

<Not disclosed>