



# CYBER RESILIENCE TASK FORCE

## Terms of Reference

*This page is intentionally left blank*

## CONTENTS

1. OBJECTIVES .....	4
2. AUTHORITY .....	4
3. REPORTING .....	4
4. MEMBERSHIP AND COMPOSITION.....	4
5. TERMS OF OFFICE .....	5
6. SECRETARIAT .....	5
7. MEETINGS.....	5
8. QUORUM .....	5
9. RELATED EXTERNAL DOCUMENTS.....	5
10. DURATION .....	5

## 1. OBJECTIVES

The Cyber Resilience Task Force (CRTF) is charged by the Profession Advisory Board (PAB) to provide recommendations in regard to certification and accreditation of educational products related to Cyber Security, including:

- Consider the potential issues in accrediting Cyber Security degrees such as criteria for universities, what would constitute such a degree, requirements for expertise of teaching staff etc;
- Ensure recommendations are aligned with international best practice and comply with appropriate national and international Cyber Security professional and educational standards;
- Review the current processes and requirements for CT/CP (Cyber) certification;
- Provide Advice regarding the process that universities would be required to go through to have their degrees listed on the ACS Cyber Security Courses webpage;
- Provide advice for future processes and structure of Specialisms based on the experience from the first two Specialisms (Cyber Security and Safety Critical Systems) pilot programs.

The Task Force activity will be in-line with members' expectations, best practice and regulatory compliance; and appropriate to a Professional Society and the Professional Practice of ICT.

## 2. AUTHORITY

2.1 The Task Force has authority to provide recommendations relating to the Cyber Security Specialism and Accreditation of Cyber Security degrees, and on the future processes and structure of Specialisms to the PAB.

2.2 The Task Force shall undertake such activities within the scope of its primary functions that it determines are required to achieve its objects.

2.3 The Task Force has no executive powers.

2.4 The Task Force cannot:

- Alter its Charter;
- Operate outside the Society's approved budget;
- Fill its own vacancies or create sub committees;
- Enter into any arrangements that legally bind the ACS.

## 3. REPORTING

The Task Force will regularly report on the business of the Task Force as set down by the PAB.

## 4. MEMBERSHIP AND COMPOSITION

4.1 The Task Force comprises up to 6 members appointed by Management Committee (MC):

- Chair, appointed by MC on the recommendation of the Director, PAB and the VP, Membership Boards;
- Up to five members with relevant background and experience
- The Director of Professional Standards & Assessment Services or delegate as a non-voting member.
- The Director, Cyber Resilience Initiatives as an attendee.

4.2 The Director of the PAB and any national officer of the ACS may attend any meeting of the Task Force.

4.3 All members shall be members of ACS.<sup>1</sup>

---

<sup>1</sup>If a Task Force nominee is not an ACS member, they may be made an honorary member with approval of the MC for the duration of their appointment to ensure appropriate expertise is available to the Task Force. It is preferable that nominees are willing to join the ACS as a member.

4.4 Task Force nominees may be sought from amongst members with expertise in the area of interest of the Task Force to assure that the appropriate quality of advice is given to the PAB.

4.5 In the event that suitable Task Force nominees are not available through the existing ACS membership, then they may be sourced from non-members.

## **5. TERMS OF OFFICE**

Members of the Task Force are appointed for the duration of the taskforce.

## **6. SECRETARIAT**

Secretariat support will be provided to the Task Force as follows:

- Meeting co-ordination including minute taking and distribution, preparation and dissemination of relevant documents, transport, accommodation, video conferencing, IT support, processing of expense reimbursement, and any other operational aspects of meetings; for general Task Force meetings and also for relevant meetings with the PAB.
- Assistance with the operational aspects of preparing documentation format for recommendations, activities and initiatives in a suitable form for the consideration by the PAB.
- Supply software licenses and any required technical support for the Board to discharge its duties.

## **7. MEETINGS**

7.1 The Task Force shall conduct face to face or videoconference meetings as deemed appropriate.

7.2 The Task Force shall operate within the approved budget for the PAB, together with any additional funds which MC may allocate to the taskforce.

7.3 Finalised agendas, supporting documentation, papers and reports are to be distributed at least 7 days prior to each meeting.

7.4 Minutes for the meeting will be prepared by the secretariat and approved by members following the meeting.

7.5 Copies of sensitive documents (in paper and electronic form) retained by the Task Force members and others assisting on their behalf should be appropriately secured to protect the privacy of any personal information and the confidentiality of the business information contained therein.

## **8. QUORUM**

A quorum is a majority of members.

## **9. RELATED EXTERNAL DOCUMENTS**

The following documents are referenced:

- PAB Terms of Reference
- ACS Declaration of Conflict of Interest
- ACS Deed of Confidentiality

## **10. DURATION**

The Task Force will be initiated within one month of approval by MC and will conclude no later than twelve months after approval by MC.

## Cyber Resilience Task Force Terms of Reference

### Authors

Ian Londish
-------------

### Version History

Date	Document Version	Revision History	Author /Reviser
26 April 2018	V0.1	Draft	Ian Londish
7 May 2018	V0.2	Edits for clarification	Nick Tate
28 May 2018	V0.3	Minor edits	Michael Johnson Nick Tate
4 June 2018	V0.4	Minor edits	PAB members
3 Sept 2018	V1.0	Varied Objectives	MC
10 Sept 2018	V1.1	Minor Edit – 1 <sup>st</sup> objective and membership	Co Secretary

### Approvals

This document requires the following approvals.

Name	Title	Date of Issue	Version
Profession Advisory Board		28 May 2018	V0.3
Management Committee		3 Sept 2018	V1.1

### Distribution

This document has been distributed to:

Name	Title	Date of Issue	Version

<b>Custodian title &amp; e-mail address:</b>	Ian Londish, Company Secretary <a href="mailto:Ian.Londish@acs.org.au">Ian.Londish@acs.org.au</a>
<b>Responsible Business Group:</b>	Governance
<b>Distribution: Highlight which is applicable and provide names where applicable</b>	



## **Cyber Resilience Task Force – Proposed Member Biographies**

### **Professor Matthew Warren (Chair)**

Matthew Warren is a Professor of Cyber Security at Deakin University and Deputy Director of the Deakin University Centre for Cyber Security Research and Innovation.

Professor Warren is a researcher in the areas of Cyber Security and he has authored and co-authored over 300 books, book chapters, journal papers and conference papers. He has received numerous grants and awards from national and international funding bodies, such as Australian Research Council (ARC); Engineering Physical Sciences Research Council (EPSRC) in the UK; National Research Foundation in South Africa and the European Union. He is a research theme leader in the CyberSecurity CRC (Cooperative Research Centres) a partnership between academia, industry and government. The CyberSecurity CRC is the biggest investment in Australian Cyber Security R&D at \$140 million dollars over seven years.

Professor Warren gained his PhD in Information Security Risk Analysis from the University Of Plymouth, United Kingdom and he has taught within Australia, Finland, Hong Kong and the United Kingdom. Professor Warren is a Fellow of the Australian Computer Society.

### **Professor Michael Johnson**

Michael Johnson has been Professor of Mathematics and Computer Science at Macquarie University since 2002. He is also a Director of the Macquarie-DEC ICT Innovations Centre and a Director and Deputy Treasurer of Dunmore Lang College. Formerly he was the Head of the Department of Computing (1997-2000) and he served as Vice-President and Chair of the University's Academic Senate (2006-2008). In 1997 he was runner up for the inaugural Australian Award for University Teaching in all Science disciplines and he has held continuous ARC large/discovery grant funding for over 20 years.

### **Emeritus Professor William J (Bill) Caelli, AO**

Bill Caelli - Retired Director of cybersecurity consultancy company IISec Pty Ltd, Emeritus Professor of the Queensland University of Technology (QUT), Adjunct Professor at Griffith University and Advisor to the School of Business and Tourism at Southern Cross University. Chairs the Safety and Stability Advisory Committee of Australia's Domain Name Authority (auDa).

Former member of the board of the "Colloquium for Information Systems Security Education (CISSE)", USA (URL <http://www.cisse.info>) from 2004 to 2013. Founder of Electronics Research Australia Pty Ltd, then ERACOM Pty Ltd, in 1979 which developed/manufactured a range of computers based on Stanford University Network (SUN) architecture with added cryptographic hardware/software. Cryptographic subsystems / security modules for IBM/clone PC, mainframes and data networks/computer security products with a first hardware encryption system for the IBM PC (1984) with full hard disk encryption/trusted key management. Founding Director of the Information Security Research Centre (ISRC) at QUT in 1988, then Head of the School of Data Communications/School of Software Engineering and Data Communications. He was made an Officer in the Order of Australia in 2003. He has over 52 years' experience in ICT with over 42

years in all aspects of cybersecurity, commercial cryptography and public policy concerns in the area. Worked for Hewlett-Packard Company and Control Data Corporation. PhD in nuclear physics / high speed data acquisition via IBM 1800/System 360/50 DACS combination.

Fellow of the Australian Computer Society (ACS), Life Senior Member of the IEEE, Fellow of ISC2, Hon CISM (ISACA), Member IFIP TC-11

Specialties: cybersecurity, network / information security & assurance, policy in cybersecurity & ICT industry, cyberwarfare/conflict/defence, cybersecurity education, SCADA/DACS security, trusted systems, SELinux, Trusted/CMW Solaris, Trusted XENIX, Trusted UNIX, SEVMS.

### **Professor Richard Buckland**

Professor Richard Buckland is the Director of First Year Experience at UNSW. He also heads the UNSW Security Engineering Capability initiative. He is Grand Challenge Visiting Professor in Cyber Security at Taylor's University Malaysia and Visiting Professor in Online Education at the National University of Malaysia.

Richard heads the applied cyber security education programme in Computer Science and Engineering at the University of New South Wales and is the director of the multi-million-dollar cybersecurity partnership with CBA. The cybersecurity students from this programme have been highly successful: they have been worldwide grand finalists at both the DEFCON and SECUINSIDE CTFs and UNSW has won the national CyberSecurity Challenge Australia competition each year since it started in 2012.

Richard has a passion for open education and for empowering students to love learning. His work as an educator has been recognised by numerous teaching awards at national and international level across several disciplines including the 2008 Australasian Engineering Educator of the Year and the 2013 Australian ICT Educator of the Year, as well as numerous teaching awards including from the Australian College of Educators and the Australian Learning and Teaching Council.

### **Lieutenant Colonel Lisa Davidson**

Lieutenant Colonel Lisa Davidson has over 27 years' experience as a Soldier and an Officer. In her career to date, she has been employed in a range of postings which involved the establishment of communications networks at the tactical, operational and strategic levels. Her service has involved deployments to East Timor, Iraq and the Middle East in both Communications and Electronic Warfare roles. She has commanded a Squadron of personnel of over 120 personnel, which she considers the highlight of her career. In recent years she has been employed in personnel management regarding Career Management of Army Officers and the management of all personnel activities of the Australian Defence Force's deployed forces.

Lisa holds a Master of Science in Information Technology and Master of Military Studies in Political Science and Government. In 2016 she was awarded the Chief of Army's Scholarship to provide a year to focus on her research at UNSW and is currently completing a Ph.D. in Cyber Security regarding Workforce Design for the Australian Army. Lisa has also presented at conferences such as the European Conference on Cyber warfare and Security.