



ACSP Program and UK Cyber Security Council

Collaboration to-date

26th April 2023

Our collaboration

The UK and Australia are leading the move towards professionalisation of cyber security globally.

Therefore the respective program teams from industry and government are meeting regularly to share learnings and updates to ensure interoperability across the schemes.

This ongoing collaboration has enabled both programs to leverage each other's learnings, resources and relationships.

Who is involved:

s22

s22

Goal / vision



Australian Cyber Security Professionalisation program goal

Improve government, business and community **trust and confidence** in Australian cyber security professionals in order for the ecosystem to continue to grow

Photo by Anna Savelle on Unsplash

AustCyber
Part of the Stone & Chalk Group



VISION

To create a world where the whole of society is safe and secure in cyber space

MISSION

To enhance and expand the nation's cyber skills, knowledge and profession at every level

UK CYBER SECURITY COUNCIL

Similarities and differences

Australia (proposed model)

- Industry and government collaboration
- Not-for-profit status
- Individuals obtain professional recognition
 - Tiered model being considered
- Disciplines / specialisms to be defined
- Governing body authorises entities to provide professional recognition to individuals
- ISACA, (ISC)² involved as authorised members
- CIISEC, SFIA, NICE skills frameworks being included

United Kingdom (in pilot)

- Industry and government collaboration
- Charity status
- Individuals obtain Chartership
 - 3 titles – Associate, Principal, Charter
- 16 Cyber Security Specialisms
- UK Cyber Security Council authorises entities to provide chartership to individuals as licenced bodies
- ISACA, (ISC)² involved as licensed bodies
- CIISEC, SFIA, NICE skills frameworks being included

Department of Industry, Science, Energy and Resources

Deed of Variation

Commonwealth of Australia (**Commonwealth**)

Australian Cyber Security Growth Network Limited
ABN 73 616 231 451 (**Growth Centre**)

Details

Date

07 1 April 1 2022
day month year

Parties

Name The Commonwealth of Australia as represented by the Department of Industry, Science, Energy and Resources

ABN 74 599 608 295

Short form name **Commonwealth**

Address details Postal address

General Manager,
Industry Growth Division,
Department of Industry, Science, Energy and Resources
GPO Box 2013 Canberra ACT 2601

Physical address

Industry House
10 Binara Street Canberra City, ACT 2601

Name Australian Cyber Security Growth Network Limited

ABN 73 616 231 451

Short form name **Growth Centre**

Address details **s22**

Postal Address

Suite 2, Level 4

AMP House

1 Hobart Place

CANBERRA ACT 2600

Background

- A On 12 December 2016, the Commonwealth and the Growth Centre entered into the Industry Growth Centre Initiative Funding Agreement (the Contract). Under the Contract, the Commonwealth provides funding for the operation of the Growth Centre. The parties varied the Contract by Deed of Variation on 04 February 2019, by exchange of letters on 7 February 2020, by Deed of Variation on 23 February 2021, by exchange of emails dated 25 March 2021 and by Deed of Variation on 8 March 2022.
- B The Commonwealth and the Growth Centre have agreed to vary the terms of the Contract in accordance with this Deed.
- C The parties acknowledge that this Deed satisfies all requirements in the Contract for a legally binding variation.

Table of Contents

Details	2
Agreed terms	5
1. Defined terms and interpretation	5
2. Variation to Contract	5
3. Affirmation of Contract	5
4. Costs and GST	5
5. Miscellaneous	5
Signing page	7
Schedule 1 – Variation to Contract	8

Agreed terms

1. Defined terms and interpretation

1.1 Defined terms

In this Deed, unless the contrary intention appears:

- (a) a word or expression defined or referred to in the Contract has the meaning given to it in the Contract;
- (b) **Contract** means the contract described in paragraph A of the Background;
- (c) **Deed** means this deed, including all annexures and schedules to it; and
- (d) **Effective Date** means the date the Deed has been executed by both parties.

2. Variation to Contract

On and with effect from the Effective Date, the Contract is varied as set out in Schedule 1 to this Deed.

3. Affirmation of Contract

- (a) The parties affirm in all other respects the covenants and conditions in the Contract as varied by this Deed.
- (b) The Contract, as varied by this Deed, comprises the entire agreement between the parties.
- (c) The parties acknowledge and agree that the Contract as varied by this Deed is and continues to be in full force and effect.

4. Costs and GST

- (a) Each party must meet or pay its own costs and expenses in respect of the preparation, negotiation, execution and completion of this Deed.
- (b) If GST is payable on any supply made under or in connection with this Deed, the recipient of the supply must pay to the supplier an additional amount equal to the GST payable on the supply provided that the supplier has given the recipient a tax invoice for the supply.
- (c) The Growth Centre must pay any stamp duties and registration or other fees (including fines, penalties and interest relating to such duties and fees) which are payable or are assessed by a relevant government body or other person to be payable in relation to this document or any transaction contemplated by it.

5. Miscellaneous

5.1 Counterparts

This Deed may be executed in counterparts. All executed counterparts constitute one document.

5.2 Governing law and jurisdiction

This Deed is governed by the law of the Australian Capital Territory and each party irrevocably submits to the non-exclusive jurisdiction of the courts of the Australian Capital Territory.

Signing page

EXECUTED as a deed.

Signed for and on behalf of the
Commonwealth of Australia as
represented by the Department of
Industry, Science, Energy and Resources
by its duly authorised delegate in the
presence of

s22

Name of witness (print)

← s22 →

Name of delegate (print)

Head of Division

Position of delegate (print)

07/04/2022

Date (print)

Executed by Australian Cyber Security
Growth Network Limited ABN 73 616 231
451 in accordance with Section 127 of the
Corporations Act 2001 in the presence of

s22

Name of director (print)

←

Signature of director/company secretary/sole director
and sole company secretary
(Please delete as applicable)

←

Name of director/company secretary/sole director and
sole company secretary (print)

06 / 04 / 2022

Date (print)

Schedule 1 – Variation to Contract

1.1 Background is varied

Background is varied by inserting the following paragraph after DA:

DB. MYEFO 2021-22 included \$18.8 million to support the transition of the Industry Growth Centres in accordance with their transition plans and Government priorities. The disbursement of the funding across Growth Centres has been approved for **exclusive use** on agreed transition activities as outlined in Item 3 of Schedule 2.

1.2 Item 3 of Schedule 2 is varied

Item 3 of Schedule 2 is varied by inserting a new row into the milestone table as 5c:

	Milestones	Milestone/Due date
5c.	Support of Transition Plan activities - A national cyber security accreditation body is established using the allocated s47(1)(b) transition funding - s47(1)(b)	30 June 2023

1.3 Item 3 of Schedule 2 is varied

Item 3 of Schedule 2 is varied by deleting the table entitled "Year 6 – 2021-22" and inserting the following after the table entitled "Year 5 – 2020-21":

Year 6 – 2021-22

Milestone	Submission Date By	Payment Date By	Payment number
Quarterly Progress Report and Quarterly Report (Q4) – 1 April – 30 June 2021	31 Jul 2021	31 Aug 2021	20
Submission of Transition Plan and 2021-22 Business Plan	30 September 2021	n/a	n/a
Quarterly Progress Report and Quarterly Report (Q1) – 1 July – 30 Sept 2021	31 Oct 2021	30 Nov 2021	21
2020-21 Annual Report			
Quarterly Progress Report and Quarterly report (Q2) – 1 Oct – 31 Dec 2021	31 Jan 2022	31 Mar 2022	22
Transition Plan updated for 2022-23	30 April 2022	31 May 2022	23

Quarterly Progress Report and Quarterly Report (Q3) – 1 Jan– 31 March 2022			
Updated Sector Competitiveness Plan	29 June 2022	n/a	n/a

Year 7 – 2022-23

Milestone	Submission Date By	Payment Date By	Payment number
Quarterly Progress Report and Quarterly Report (Q4) – 1 April – 30 June 2022	31 Jul 2022	n/a	n/a
Quarterly Progress Report and Quarterly Report (Q1) – 1 July – 30 Sept 2022	31 Oct 2022	n/a	n/a
2021-22 Annual Report			
Quarterly Progress Report and Quarterly report (Q2) – 1 Oct – 31 Dec 2022	31 Jan 2023	n/a	n/a
Quarterly Progress Report and Quarterly Report (Q3) – 1 Jan– 31 March 2023	30 April 2023	n/a	n/a
Quarterly Progress Report and Quarterly Report (Q4) – 1 April – 30 June 2023	30 June 2023	n/a	n/a

Transition Activities

The Growth Centre will implement the transition activities that are outlined in the Transition Plan and that have been approved (in advance) by the Commonwealth (**Transition Activities**). Depending on the scope of the Transition Activities, the Growth Centre may be required to submit a budget related to the Transition Activities to the Commonwealth for prior approval. All Transition Activities are to be completed in accordance with the Transition Plan or as otherwise agreed between the parties and must be completed no later than the End Date.

1.4 Item 1 of Schedule 4 is varied

Item 1 of Schedule 4 is varied by deleting it in its entirety and replacing it with the following:

The total amount of the Funds is **s47(1)(b)** (*excluding* GST).

Subject to the terms of this Agreement, the Commonwealth will pay the Funds to the Growth Centre in the instalments set out in the following schedule.

Milestones	Funding Amount	GST	Total (GST inclusive)
Payment 1 - on Execution	s47(1)(b)		
Payment 2			

Milestones	Funding Amount	GST	Total (GST inclusive)
Payment 3	s47(1)(b)		
Total 2016-2017			
Payment 4			
Payment 5			
Payment 6			
Payment 7			
Total 2017-2018			
Payment 8			
Payment 9			
Payment 10			
Payment 11			
Total 2018-2019			
Payment 12			
Payment 13			
Payment 14			
Payment 15			
Total 2019-2020			
Payment 16			
Payment 17			
Payment 18			
Payment 19			
Total 2020-2021			
Payment 20			
Payment 21			
Payment 22			
Payment 23			
Payment on <u>30 April 2022</u> for Transition Plan activities being those			

Milestones	Funding Amount	GST	Total (GST inclusive)
activities described in 5c of the table in Item 3 in Schedule 2	s47(1)(b)		
Total 2021-2022			
TOTAL PAYMENTS Year 1-6			



Audit Trail

TITLE	AustCyber Deed of Variation - April 2022
FILE NAME	AustCyber - Deed ...ril 2022.docx.pdf
DOCUMENT ID	cb38b9b25503da44103eb051aaefef974a0401b0
AUDIT TRAIL DATE FORMAT	DD / MM / YYYY
STATUS	● Signed

Document History



06 / 04 / 2022
13:22:30 UTC+10

s22



06 / 04 / 2022
15:29:25 UTC+10

s22



06 / 04 / 2022
15:29:40 UTC+10

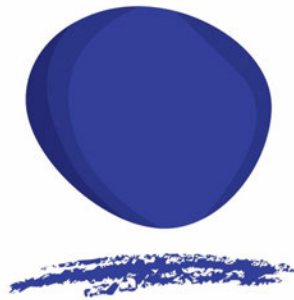
s22



COMPLETED

06 / 04 / 2022
15:29:40 UTC+10

The document has been completed.



AustCyber

Part of the Stone & Chalk Group

Quarterly Report

1 July 2023 to 30 September 2023

Australian Cyber Security Growth Network Limited
to
Department of Industry, Science and Resources

Australian Cyber Security Growth Network Ltd
An Australian Government Industry Growth Centre
Unit 2, Level 4, 1 Hobart Place, Canberra City ACT 2601
ABN 73 616 231 451

S22

S22

S22

c. Skills building activities

Australian Cyber Security Professionalisation Program (ACSP)

During this reporting period:

- Phase one was completed and the final draft Phase 1 report, including the proposal for phase 2 was completed and provided to Government partners in mid July for further feedback/review.
- Ongoing collaboration continues with key partners and stakeholders in preparation for the next phase of the program
- Introductions and briefings with new stakeholders to learn, share and identify opportunities for collaboration and input in the next phase including:
 - Skills Framework for the Information Age (SFIA)
 - Canberra Cyber Hub – Tertiary Education taskforce
 - Standards Australia
- Continued discussions with DISR, ACSC, Home Affairs and the Cyber Security Strategy team around the plan and timeline for phase 2.
- AustCyber participated in and supported the Hudson (member of AIIA) breakfast event *Cyber Security Professionalisation in Australia* held in Canberra on Wednesday 20th September.

Canberra event overview

AustCyber participated in the Hudson (AIIA member) hosted breakfast and workshop event focused on *Cyber Security Professionalisation in Australia* held in Canberra on Wednesday 20th of September.

This event attracted over 40 attendees across government and the cyber security sector and included an overview of the ACSP program, a panel discussion about professionalisation and a workshop session encouraging participants to share their ideas and thoughts to help shape the next phase of the program.

The panel featured:

s22

- s22

Stakeholder engagement

The following meetings and briefings occurred with program stakeholders:

- Co-design team
 - Adhoc individual briefings with team members to provide updates and capture input and feedback on program decisions and outcomes
 - ACS & Canberra Cyber Hub, 3 August - ACSP program overview and sharing session
 - ACSP co-design session, 7 August - phase 2 planning
 - Insurance Council of Australia, 10 & 15 August - ICA cyber security working group program update and sharing session
 - ACS, 30 August - program update
 - ACS & Canberra Cyber Hub, 6th September - program overview and participation in Tertiary Education Sector Collaboration Taskforce meeting focused on cyber security workforce challenges
 - Co-design team & UK Cyber Security Council, 20 September - Uk 'lessons learned' sharing session
- Government briefings and engagement
 - Investment NSW, 21 July - contributed to the NSW Cyber Security Skills Framework focus group session
 - DISR, 31 July - discussion including ongoing awareness raising and phase 2
 - DISR, 15 August - phase 2 plan and timeline discussion with co-design team
- Industry stakeholders
 - SFIA, 4 July - sharing session and walkthrough of SFIA framework
 - UK Government & Council, 4 July - program update and sharing/learning session
 - Standards Australia, 20 July - sharing session
 - Fifth Domain, 8 August - program update and phase 2 opportunities
 - DSO/FSO, 10 August - participate in Workforce Plan workshop
 - IOT, 11 August - program update
 - Engineers Australia, 18 August - ongoing engagement to share and collaborate on respective programs of work to ensure consistency where relevant.
 - FSO & APSC, 25 August - sharing session to identify collaboration opportunities across related programs of work.

- Hudson, ACS & NACC, 20 September - exploring collaboration opportunities for phase 2

Program Promotion

In July, FAQs approved by the co-design team were added to the ACSP webpage. These are created to increase SEO for the webpage as well as to provide further clarity to audiences about professionalisation and what the program entailed.

The breakfast held in Canberra during September was also promoted on socials, with co-design team members who were part of the event being tagged in social posts reflecting upon the event.

Work began in September on a case study showcasing the impact of the co-design approach. It will be released and promoted during the next quarter across AustCyber and Stone & Chalk channels.

s22

S22

S22

S22

b. Key transition milestones

s22

[Redacted]	
[Redacted]	

Australian Cyber Security Professionalisation (ACSP) program

Current status overview	Please refer to the detailed ACSP program update under c. Skills building activities above Estimated 100% complete (phase one)
Key activities completed in period (max 5)	- Delivered final draft phase 1 report which included the phase 2 proposal to DISR, Home Affairs and ACSC for feedback - Participated in the Hudson event Cyber Security <i>Professionalisation in Australia</i> held in Canberra on Wednesday 20th September.

s22

S22

S22

S22

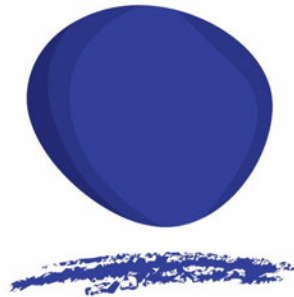
S22

S22

S22

S22

S22



AustCyber

Part of the Stone & Chalk Group

Quarterly Report

1 October to 31 December 2022

Australian Cyber Security Growth Network Limited
to
Department of Industry, Science, Energy and Resources

Australian Cyber Security Growth Network Ltd
An Australian Government Industry Growth Centre
Unit 2, Level 4, 1 Hobart Place, Canberra City ACT 2601
ABN 73 616 231 451

S22

S22

S22

S22

S22

S22

S22

S22

S22

S22

S22

S22

s22

Australian Cyber Security Professionalisation Program (ACSP)

During this reporting period:

- The Accreditation Body Program name changed to the Australian Cyber Security Professionalisation (ACSP) Program to better reflect the program goal
- One-on-one interviews were conducted with co-design team members (industry experts) to learn about their career journeys and what is a 'professional'
- The second face-to-face co-design workshop was held in November

- Cyber security employee and employer qualitative research began
- NDA's were executed between AustCyber and each of the co-design team members (except AISA which we anticipate will be executed in the next reporting period) and other relevant stakeholders such as Engineers Australia and Digital Skills Organisation to allow for continued collaboration
- A shared working space has been created via Miro for the co-design team to collaborate and share resources and information throughout the life of the program
- Public announcement wording (approved by the co-design team) was drafted and submitted to s22 office for consideration to formally announce this initiative
- Numerous briefings and discussions were undertaken with relevant government agencies and industry stakeholders to continue to seek feedback and input on the outputs of this program and align with and learn from other relevant programs and projects.

Workshop overview

The second face-to-face co-design workshop was held in Canberra on 8th November 2022. This workshop was kindly hosted at the new Australian Computer Society Canberra hub and focused on designing the baseline to be recognised as a cyber security professional, identifying personas to be developed, and defining the core elements of career pathways.

The following co-design team members attended and contributed in person:

- s22 - Australian Computer Society (ACS)
- s22 - (ISC)2
- s22 - industry expert (KordaMentha)
- s22 - RMIT
- s22 - Tech Council of Australia
- s22 - Australian Information Industry Association (AIIA)
- s22 - Australian Information Security Association (AISA) - half day

The following co-design team members were unable to attend the workshop in person. They were engaged separately to provide their input to the workshop topics:

- s22 – ISACA
- s22 TAFECyber

Additional stakeholders that attended the workshop:

- s22 – Australian Public Service Commission Digital Profession (APSC) – half day

In the weeks leading up to the second workshop the program team conducted one-on-one interviews with each member of the co-design team to understand each individual's career journey and identify the common elements that define what it means to be considered a 'professional'. These insights were shared with the team at the workshop and helped to provide the team with a starting point to stimulate the discussion and seek consensus on the day.

The program team invited s22 from APSC to present to the team the APS Cyber Security Career Pathfinder tool and the current project underway to review, and where required, update/amend the disciplines, roles, levels and frameworks that inform this tool. The purpose of this opportunity was for:

- the co-design team to consider defining or agreeing on the core disciplines/roles in cyber security relevant to the Australian market,
- to ensure where possible, there is alignment with other related programs of work across the public and private sectors, and
- to learn from, leverage and provide input into other existing similar initiatives.

The remainder of the workshop focused on activities that resulted in the team working through the baseline requirements to be recognised as a professional, the elements that should be included in the development of career pathways and the approach to the customer research and what personas to be developed for employees and employers.

Workshop outcomes

- The co-design team reviewed and provided some initial feedback on the proposed updated APS Career Pathfinder disciplines for consideration. The main feedback focused on expanding the non-technical cyber security

discipline to possibly three disciplines and consolidating a couple of the technical disciplines with similar base skill requirements.

- The team hasn't at this stage achieved consensus on the cyber security disciplines or knowledge areas due to the complexity of this topic. The program team anticipates this will continue to be discussed in the next reporting period as part of the next workshop focussed on the frameworks.

The team agreed:

- the draft baseline requirements to be recognised as a cyber security professional are:
 - Demonstrate a level of expertise in cyber security
 - Undergo continuing professional development in cyber security
 - Adhere to a code of ethics

Note: further work is required to expand the detail under each of the requirements

- existing work should be leveraged to inform the core elements of career pathways
- qualitative research is to be conducted to:
 - develop the agreed employee and employer personas
 - employees - new entrant, career changer, existing worker, international worker
 - employers - corporate, government, SME non-tech, SME tech but no cyber security expertise
 - understand the needs and experience of these different personas working in cyber security and employing cyber security skills
 - inform the development of the career pathways to become or be recognised as a professional
- there is a need for a code of ethics and/or professional standard that professionals should be required to adhere to

Qualitative employee and employer persona research

The research team began this project mid November. It is expected 5 one-on-one interviews (total 40-45) will be conducted for each persona to capture the insights and data required. The ACSP co-design team were engaged to assist with

communicating this research project through their respective networks to encourage individuals that may meet the research criteria to participate.

At the end of this reporting period a total of 15 interviews were completed:

- Employees:
 - Existing worker x 4
 - Career changer x 3
 - International worker x 1
- Employers:
 - Corporates x 3
 - SME – tech but no cyber security expertise x 1
 - SME – non-tech x 2

It is anticipated this research will be completed during the next reporting period.

Stakeholder engagement

As part of the broader industry stakeholder engagement, the program team is continuing to receive opportunities to meet, share, learn from and collaborate with the leads of other related projects and programs. Through these opportunities the team:

- is working with the Digital Skills Organisation and APSC to visually represent how our respective programs align and complement each other. We anticipate this visualisation will be finalised in the next reporting period.
- was introduced via email to the CEO of UK Cyber Security Council during the Christmas break. The team will engage with the CEO in early 2023 and will provide an update on this introduction and opportunity in the next reporting period.

The following meetings and briefings occurred with program stakeholders:

- Co-design team
 - One-on-one interviews (as detailed above)
 - Individual debriefs with team members after each workshop to capture any further feedback and seek final confirmation on decisions and outcomes

- Australian Computer Society (ACS), 31 October & 16 November – share and connect on respect programs of work related to professional frameworks
- Australian Information Industry Association (AIIA), 12 & 13 December – AIIA member sharing sessions to provide overview of program and seek feedback and comments
- Tech Council of Australia, 16 November – invited to cyber security working group meeting to provide overview of program and seek feedback and comments
- Tech Council of Australia, 15 December – invited to members meeting to provide overview of program and seek feedback and comments
- Government briefings and engagement
 - Department of Employment and Workplace Relations (DEWR), 6 October – initial engagement and program overview
 - APSC Cybersecurity Career Pathfinder Workshops, 13 & 28 October – invited to contribute to these workshops and learn about the Career Pathfinder Tool project and opportunity to collaborate and provide input
 - DISR, Home Affairs, DEWR and ACSC, 10 November – second workshop debrief and feedback/input on decisions and outcomes
- Industry stakeholders
 - Engineers Australia, 21 October – introductory meeting to share and explore opportunities to collaborate. Learn about the Cyber Engineering project.
 - AustCyber Innovation Node Network, 11 November – second workshop debrief and feedback/input on decisions and outcomes
 - Digital Skills Organisation (DSO) Employer Workshop, 10 November – learn about the co-design process used to design the DSO pilot program
 - DSO, 23 & 28 November and 12 December – further sharing and understanding of the DSO skills standards and pilot program
 - UNSW Institute of Cyber Security (IFCYBER), 13 December – introductory meeting to share opportunities for collaboration related to this program
 - Engineers Australia, 16 December – regular briefing on respective programs of work.

S22

S22

S22

S22

S22

S22