S 22

From: S 22
Sent: Friday, 25 February 2022 3:19 PM
To: S 22
Cc: Digital Programs; S 22 S 22
Subject: RE: For approval: Cyber Security Skills Partnership Innovation Fund Round 2 Recommendations [SEC=OFFICIAL:Sensitive]

Hi S 22

Approval minute has been signed.

Kind regards, S 22

S 22
Manager A/g
Digital, Innovation and Space programs | Portfolio Program Delivery | AusIndustry
Department of Industry, Science, Energy and Resources
T (S 22 | **M** S 22

OFFICIAL: Sensitive

From: S 22
Sent: Wednesday, 23 February 2022 2:02 PM
To: S 22 @industry.gov.au>
Cc: Digital Programs <DigitalPrograms@industry.gov.au>; S 22 @industry.gov.au>; S 22 @industry.gov.au>
Subject: For approval: Cyber Security Skills Partnership Innovation Fund Round 2 Recommendations [SEC=OFFICIAL:Sensitive]

Good afternoon S 22

For approval please see below the approval minute for the Cyber Security Skills Partnership Innovation Fund Round 2 Recommendations.

Approval Minute

Once approved we will send you the Ministerial brief regarding the announcement of successful grantees.

Thank you
S 22

S 22
Program Manager

AusIndustry | Portfolio Program Delivery | Digital, Innovation and Space Programs
Ngunnawal Country, Industry House, 10 Binara Street (GPO Box 2013) Canberra ACT 2601 Australia
Department of Industry, Science, Energy and Resources
P S 22 @industry.gov.au

business.gov.au 13 28 46 (8am - 8pm local time, Monday to Friday)
Subscribe to news updates

industry.gov.au ABN 74 599 608 295

MINUTE

Australian Government
Department of Industry, Science, Energy and Resources

AusIndustry

S 22

Manager / Program Delegate
AusIndustry
Department of Industry, Science, Energy and Resources

For Action by 2 March 2022

SPENDING PROPOSAL: PROVISION OF $25,406,811 (PLUS GST WHERE APPLICABLE) TO THE CYBER SECURITY SKILLS PARTNERSHIP INNOVATION FUND ROUND 2.

RECOMMENDATION

1. That you, in accordance with the Department of Industry, Science, Energy and Resources (department) Delegations and consistent with the grant opportunity guidelines and relevant departmental policies:

    a) make, vary or administer an arrangement or grant for the **Cyber Security Skills Partnership Innovation Fund Round 2** in accordance with sections 34 and 35 of the *Industry Research and Development Act 1986* (IR&D Act) in relation to prescribed programs, including to spend relevant money and other CRF money, as the expenditure is supported by an instrument under s33 of the IR&D Act.

2. That you agree with the substantive reasons for the spending proposal provided below in accordance with Accountable Authority Instructions (AAI) 2 and that the spending proposal would be an efficient, effective, economical and ethical use of Commonwealth resources that is not inconsistent with the policies of the Australian Government.

Reasons for the spending proposal (AAI 2)

The Cyber Security Skills Partnership Innovation Fund Round 2 (the Program) Grant Opportunity Guidelines (**Attachment A**) were released on 25 October 2021 when applications for the Program opened. Applications for the Program closed on 6 December 2021.

40 applications were received for the Program, these were all deemed eligible against the Grant Opportunity Guidelines and progressed the merit assessment process which was conducted in accordance with the agreed framework. The recommended successful applicants were competitive against the relevant merit criteria established for the Program.

The merit assessment process was undertaken by an Assessment Committee made up of Australian Government representatives. The Assessment Committee met on 3 February 2022 and 11 February 2022 to discuss and moderated applications, determining the final scores and recommendations.

Recommendation summary:

Application number	Applicant name	Grant amount
S 22		
CSSIII000008	FIFTH DOMAIN PTY LTD	$3,000,000
S 22		

Total Recommended Applications	$25,406,811

The Assessment Committees full recommendations are at **Attachment B**.

Background/Summary

The $70.3 million Cyber Security Skills Partnership Innovation Fund forms part of Australia's Cyber Security Strategy 2020, Cyber Security National Workforce Growth Program, and was developed in recognition that skilled cyber professionals are essential for keeping Australians secure online, and to underpin government and industry capability and capacity.

The objectives of the Program are to:

- increase diversity in the cyber security workforce
- the creation of new and innovative ways to improve the quality and quantity of cyber security professionals in Australia
- improve collaboration between industry and the education sector to build the quality and availability of cyber security professionals in Australia support industry and academia to attract, train and place cyber security talents into their businesses

The intended outcomes of the Program are:

- increased diversity of the cyber security workforce including lifting the participation of women, Indigenous Australians, regional and remote based workers, and neuro diverse individuals
- delivering a pipeline of highly skilled cyber security professionals to meet with the current and future need of Australia's digital economy
- enhanced Australia sovereign cyber security capability to underpin our growing digital economy and the safety of all Australians

Any future year expenditure

- The spending proposal will include expenditure in forward years. The breakdown of the spending proposal across all relevant financial years is:

	2021/22	2022/23	2023/24	Total
	(GST excl)	(GST excl)	(GST excl)	(GST excl)
Appropriation	$24,307,000	$23,000,000	$21,000,000	$68,307,000
Current Commitments	$2,877,284	$3,288,326	$2,055,203	$8,220,814
Funds Available for Round 2	$21,429,716	$19,711,647	$18,944,797	$60,086,187
Spending Proposal Round 2	$6,575,771	$12,407,133	$6,423,907	$25,406,811
Uncommitted Funds after Spending Proposal	$14,853,945	$7,304,514	$12,520,890	$34,679,376

- In approving this spending proposal you are also approving any additional amounts associated with the GST component for the grants.

Any potential criticisms and risks of significance

- The Policy owner for the Program is concerned there may be criticism that not all applications received funding when there was enough budget available to do so.
- There is a risk to $14,853,945 in funding if a Movement of Funds is not approved at the end of this Financial Year, which will impact the amount of funding available for Round 3 of the Program. The Policy owner is aware of this risk.

Any conditions on the approval

- All eighteen recommended projects will entail a condition of funding stating “A formal arrangement must be in place with all project partners prior to execution of the grant agreement”.
- Additional conditions to funding to specific projects are outlined at Attachment A (the Committee Chair letter to Delegate – Applications Highly Suitable/Suitable and Recommended for Funding).
- All conditions will be addressed in the letters of offer and during the grant agreement negotiation process.

PGPA Act - s60 - Contingent Liabilities

- There are no identified contingent liabilities associated with this spending proposal.

Attachments

A. Grant Opportunity Guidelines
B. Committee Chair letter to Delegate, including:
   a. Meeting Minutes
   b. Application scoring form template
   c. Merit Assessment Framework
   d. Applications Highly Suitable/Suitable and Recommended for Funding
   e. Applications Suitable but Not Recommended for Funding
   f. Applications Not Suitable and Not Recommended for Funding

S 22

Program Manager
Digital Program

23 February 2022

Decision	
Spending proposal: PROVISION OF $25,406,811 (PLUS GST WHERE APPLICABLE) TO THE CYBER SECURITY SKILLS PARTNERSHIP INNOVATION FUND ROUND 2.	**Agreed**/~~Not agreed~~
Substantive reasons	**Agreed**/~~Not agreed~~
S 22 Program Delegate	S 22 Signature
Date:	25/02/2022

Australian Government
Department of Industry, Science, Energy and Resources

AusIndustry

Cyber Security Skills Partnership Innovation Fund Round 2 Committee Recommendations

S 22

Program Delegate
Cyber Security Skills Partnership Innovation Fund Round 2
Department of Industry, Science, Energy and Resources
CANBERRA ACT 2601

Dear S 22

Cyber Security Skills Partnership Innovation Fund Program Round 2 (Program) Recommendations

As Chair of the Cyber Security Skills Partnership Innovation Fund Round 2 Committee, I recommend 18 projects to proceed to the next stage of the Cyber Security Skills Partnership Innovation Fund Round 2 (Program) to be approved by you, as the responsible Program Delegate for this Program.

The Program Committee (the Committee) met on Thursday, 3 February 2022, and Friday, 11 February 2022, to deliberate on 40 eligible applications received under the Program. Please see meeting minutes at **Attachment A**.

Prior to the meeting, the Committee members were allocated up to eight applications each to assess as a primary assessor or secondary assessor. An application scoring form (**Attachment B**) and data spreadsheet were developed to assist members score and rate applications assigned to them. A Merit Assessment Framework (**Attachment C**) was developed by the Program Team and provided to the Committee to ensure all applications were assessed equally.

The Grant Opportunity Guidelines (Guidelines) stipulate that applications must score highly against each merit criterion to be considered for funding. The Committee agreed that in line with the Guidelines and Merit Assessment Framework applications that scored 68 or less by both the primary and secondary assessors were considered unsuitable for funding, and as such, were not going to be discussed. There were 16 applications in this category.

The Committee took into consideration the merit of the remaining applications and evaluated them against the assessment criteria. Final scores and recommendations for these applications were agreed on.

The Committee agreed that in line with the Guidelines and Merit Assessment Framework applications that scored 84 or above would be Recommended for Funding as they ranked Highly Suitable.

The Committee agreed that in line with the Guidelines and Merit Assessment Framework applications that scored 75-83 would be Recommended for Funding as they ranked Suitable and met the intended objectives and outcomes of the Program. These applications showed the applicant could deliver the project and represented value for money.

A full list of applications that were assessed to be Highly Suitable or Suitable and recommended for Funding is at **Attachment D.**

The Committee agreed that in line with the Guidelines and Merit Assessment Framework applications that scored 69-74 would Not be Recommended for Funding as while Suitable for consideration by the Committee the applications lacked relevant detail, evidence or reasoning. The weaknesses of these applications outweighed the strengths and they did not represent value for money. Applications rated Suitable but Not Recommended for Funding are at **Attachment E.**

Applications rated 68 or below were deemed Not Suitable and Not Recommended for funding, these are listed at **Attachment F**.

The Committee endorsed the following 18 projects as suitable and recommended for funding.

Score	Application number	Applicant name	Grant amount
S 22			
86	CSSIII000008	FIFTH DOMAIN PTY LTD	$3,000,000
S 22			
Total Recommended Applications			$25,406,811

These recommendations are below the available grant funds of $60,086,187. The remaining amount of $34,679,376 will be reallocated to a potential Round 3 of the Program.

The 18 recommended applicants partnered with the industry associations, employers, higher education and vocational education providers, secondary schools, and local and states businesses. These innovative projects will improve the quality and availability of cyber security professionals in Australia. The projects also will build Australia's future pipeline of skilled cyber security professionals. The applicants demonstrated the capacity and capability to carry out the project and represent value for money.

The 18 projects will entail a condition of funding stating "A formal arrangement must be in place with all parties prior to execution of the grant agreement" as per item 7.2 of the Guidelines. Additional specific conditions to funding for individual projects are outlined in **Attachment D**. All conditions will be included in the Letters of Offer sent to the Successful applicants and require applicants to meet these conditions prior to entering in to a Grant Agreement with the Commonwealth.

In my capacity as Chair of the Program's Committee, I recommend these 18 projects proceed to the next stage of the Program.

Yours sincerely,

S 22

Committee Chair
22 February 2022

Attachment A

COMMITTEE MEETING MINUTES

Australian Government
Department of Industry, Science, Energy and Resources

AusIndustry

Cyber Security Skills Partnership Innovation Fund Round 2 Assessment Committee Meeting
Thursday, 3 February 2022, 9.00am – 1.00pm AEDT
Online Meeting via Skype
Minutes

Item No	Agenda Item	Presenter
1.	**Opening and welcome** • Acknowledgement to Country • Chair thanked the Committee members and noted importance of this program and the projects it will fund.	S 22 , ***Chair***
2.	**Program Management Update** Program Manager welcomed the Committee and thanked them for their time. Brief introductions of those present: • S 22 • • • • • • • • • • • • •	S 22 ***Program Manager***

- S 22
-
-

S 22 and S 22 were apologies. S 22 was an expert panel member, however, there were no applications that the Committee sought additional assistance on assessing.

It was noted that if the Committee cannot agree on a score for based on the first and secondary assessors' comments, we will email the application to all Committee Members and break for 30 minutes to allow time for everyone to review the application and vote on a final score.

Probity discussion

- Committee reminded that the probity plan was provided electronically and discussed as part of induction
- Reminder that the Committee must follow assessment process consistently for all applicants.

Disclosures of Interest

- Committee informed that there were two Category 3 perceived Conflicts of Interests and the following people were asked not to participate and turn off their camera while these applications were discussed:
  - S 22 application CSSIII000008 S 22
- Committee asked that if they identify any additional conflicts of interest during the day to raise these with the Program Manager immediately via email or Skype

Ranking and scoring requirements

- The Guidelines stipulate that applications must score highly against each merit criterion to be considered for funding—according to the assessment framework this has been determined as scoring at least 84 and above and 68 or less is considered unsuitable for funding.
- Program Management have calculated the average score (between first and second assessor) and use this as the agreed Committee Score, unless the Committee discussion changes this and agrees to change it.
- It was noted $60.1 million in funding was available but due to receiving less than anticipated applications, just over $41.6 million was requested, we would not be tracking the available funding.
- Due to our Program Management system only accepting whole numbers all average scores have been rounded.

Demonstration of Assessment Workbook

- The Committee were provided with a workbook.
- If any other documentations were required the program team would send to the members.

	Preliminary ranking of applications • **Committee Agreed** that the average scores will be used as the final score unless specially discussed and changed by the Committee. • **Committee Agreed** that under the Merit assessment framework applications that scored 68 or less are not suitable. Where both assessors scored 68 or less the Committee would not need to discuss these applications and they will be deemed Not Suitable and Not Recommended for funding. Application numbers: S 22 • **Committee Noted** there were 15 applications in this category, leaving 25 applications to be considered. • **Committee discussed and agreed** to leave the three applications that had an average score 68 or under because one assessor scored above the benchmark and one scored below will be left in the applications to be discussed. Application numbers: S 22	
3.	**Application Assessment** • Committee commenced discussion of each application from the highest scoring. • Primary and Secondary spokesperson gave a brief overview of the application and justification to their scoring. • **Committee discussed and agreed**:	***Committee led by*** S 22 ***Chair***

	S 22 ○ CSSIII000008 – come back to score later after full committee can read the application S 22 • Program Manager noted that the discussions today was taking longer than anticipated and we would not be able to finalise all applications today. • The Committee agreed to reschedule another meeting for Friday, 11 February 2022, to finish the remaining applications as the meeting ran out of time. • **Committee discussed and agreed**: S 22 • Program Manager noted that all applications with an average score of 84 or above have been discussed.	
	Break from 11:50am - 12:00pm	
5.	**Application Assessment** • Chair noted that we have discussed all applications that are above the cut off score to be deemed Highly Suitable • Continued discussion of each application from the highest scoring. • Primary spokesperson gave a very brief overview of the application, both assessors to speak to their scoring. • **Committee discussed and agreed**: S 22	***Committee led by*** S 22 , ***Chair***

	S 22 S 22	
6.	**Meeting close at 1pm** The Program Management team to reschedule a further three hours next week to finish the remaining applications and recommendations. The Committee's preference for the next meeting was Friday afternoon, 11 February 2022.	S 22

Cyber Security Skills Partnership Innovation Fund Round 2 Assessment Committee Meeting

Friday, 11 February 2022, 1.30pm – 4.30pm AEDT
Online Meeting via **Skype**
Minutes

Item No	Agenda Item	Presenter
1	**Opening and welcome** • Chair welcomed Committee and asked Policy lead, S 22 to comment on the high level objectives of today. • S 22 reiterated to the Committee that the overarching core principals of the program are to grow the cyber workforce and create opportunity, which was to be done by funding projects that lead to growth in the cyber security workforce, strengthen partnerships and those where the organization has shown they can deliver. • These are the high level drivers and purpose of the program.	S 22 , ***Chair***
2.	**Program Management Update** • Program Manager noted that the Committee can recommend projects for funding as long as they are able to defend the recommendation that the project contributes to the objectives and outcomes of the program, the applicant can deliver and it represents value for money. • S 22 , S 22 , S 22 and S 22 were apologies. S 22 to join the meeting around 2pm. S 22 needed to leave at 3pm. • Program Manager noted the aim of today was for the Committee to agree on what applications should be recommended for funding and finalise scores for each application that reflect these recommendations. The Committee agreed to lower the benchmark from 84 to 75, however they could not recommend applications that do not score high enough to be considered as suitable for funding. • Committee reminded that the probity plan was provided electronically and they must follow assessment process consistently for all applicants. Reminder of Disclosures of Interest • Committee reminded that there were a couple of Category 3 perceived Conflicts of Interests and the following people were asked to mute and turn off their camera should these applications be discussed:	S 22 ***Program Manager***

	○ S 22 application CSSIII000008; and ○ S 22 • Committee were asked that if they identify any additional conflicts of interest during the day to raise these with the Program Manager immediately via email or Skype. • Program Manager noted applications were not listed in order of scores due to some Committee members not being able to attend all afternoon, this was not always possible to facilitate.	
3.	**Application Assessment** • Committee commenced discussion of each application left for discussion. • Primary and Secondary spokesperson gave a brief overview of the application and justification to their scoring. S 22 S 22 S 22	***Committee led by*** S 22 ***, Chair***

	S 22 • No additional applications were raised for discussion.	
	Break from 3:22pm - 3:40pm	
4.	**Application Assessment** • **Committee discussed and agreed** to lower the benchmark score for those applications that will be recommended for funding to 75. • Committee commenced discussion of applications previously discussed where a final score was not agreed. • **Committee discussed and agreed**: S 22 ○ CSSIII000008 – leave average score as committee score S 22	***Committee***
5.	**Meeting close at 4.20pm** • Program Manager invited Committee members to provide any feedback on the process or assessment of applications to the Program Management team.	S 22

	• Program Manager noted that application S 22 would be emailed to Committee for review and a decision would be made via correspondence, coordinated by the Chair. • Program Manager noted that should the Program Management team require additional Strengths and Weaknesses we would be in contact. • Program Manager thanked committee.	

Post Committee Meeting:

On 11 February 2022, the Program Management team emailed the Committee members application S 22 for further consideration and reassessment.

On 14 February 2022, Committee Chair S 22 asked the Committee to support this application for funding out of session. This was agreed.

ATTACHMENT B

APPLICATION SCORING TEMPLATE

Cyber Security Skills Partnership Innovation Fund Round 2

Committee Application Assessment

Application details

Application number	{Program Management Insert Application number}
Applicant organisation name	{Program Management Insert Organisation name}
Grant amount sought	{Program Management Insert Grant amount}
Primary assessor score	XX /100
Secondary assessor score	XX /100
Committee member (primary assessor)	{Program Management Insert Primary Assessor's name}

Assessment against the assessment criteria

Refer to the ***Assessment Scoring Framework*** for guidance on scoring each criterion. The following table should be used for guidance on the overall rating. Only applications assessed as highly suitable or suitable should be considered to recommend for funding.

Highly Suitable (84 or more)	Overall, the applicant has provided a strong application whereby the assessment criteria has been addressed to a very high standard. The information provided is clear, convincing and comprehensive, and is generally supported by a thorough analysis and evidence.
Suitable (69 to 83)	Overall, the applicant has provided a satisfactory to good application whereby the assessment criteria has been addressed to a satisfactory to good standard. The information provided is clear but lacking detail. The information is generally supported by relevant analysis and evidence.

Not Suitable (68 or less)	Overall, the applicant has provided a marginal to poor application whereby the assessment criteria has not been addressed to a suitable standard. The information and analysis provided to address the assessment criteria may be clear in some areas but is generally limited, inadequate, unclear or irrelevant.

Primary assessment

Assessment criterion 1 - How your project will improve the quality and availability of the cyber security workforce in Australia, and how innovative it is.

Score *XX /40*

Comments

Analyse the applicant's response. Include any gaps in the response, or comment on how well the applicant has validated its claims. The applicant was required to demonstrate they meet this criterion by identifying:

- how the project will increase the quality and availability of job-ready cyber security professionals in Australia, including measures that increases the diversity of the cyber security profession, for example women, Indigenous Australians, regional and remote based workers, and neuro diverse individuals. With a focus on how the project will achieve and demonstrate this change
- how the project will help develop the cyber security workforce and meet industry needs
- the extent that the project approach is innovative (new or significantly improved – see the Glossary in the Program Opportunity Guidelines for more information).

Further information: Where relevant applicants should include evidence to support their claims against the criteria, applications with a strong evidence base will be considered more meritorious.

{Insert comments}

Assessment criterion 2 – How the delivery of your project promotes collaboration between industry and the education sector.

Score *XX /25*

Comments

Analyse the applicant's response. Include any gaps in the response, or comment on how well the applicant has validated its claims. The applicant was required to demonstrate they meet this criterion by identifying:

- the approach/methods it will use to improve collaboration between industry and the education sector
- who the key stakeholders will be and how they propose to work with each of them
- how partnerships formed to deliver your project will have a lasting impact beyond the term of grant funding

{Insert comments}

Assessment criterion 3 – Capacity, capability and resources to deliver the project.

Score *XX /25*

Comments

Analyse the applicant's response. Include any gaps in the response, or comment on how well the applicant has validated its claims. The applicant was required to demonstrate they meet this criterion by identifying:

- their track record managing similar projects and access to personnel with the right skills and experience, including management and technical staff
- their plan to manage the project, addressing scope, implementation plan, timeframes, budget and risk (including any national security risk)
- how they will measure and evaluate the success of the project
- their strategy to maintain the project outcomes beyond the term of the grant funding.

{Insert comments}

Assessment criterion 4 – Impact of the grant funding on the project.

Score *XX /10*

Comments

Analyse the applicant's response. Include any gaps in the response, or comment on how well the applicant has validated its claims. The applicant was required to demonstrate they meet this criterion by identifying:

- how the funding amount requested can be justified with respect to the scale of the project and intended outcomes
- the likelihood that the project would not proceed without the grant. How the grant will positively impact the project, for instance in terms of size, scale and timing
- any additional investment the grant will leverage and explain how this benefits the project.

{Insert comments}

Strengths and weakness of the application

Please note that feedback provided in this section will be passed on to applicants. The information must be presented in clear, concise, and complete sentences that cannot be misconstrued.

Strengths

- {Insert strength}
- {Insert strength}
- {Insert strength}

Weaknesses

- {Insert weakness}
- {Insert weakness}
- {Insert weakness}

Other considerations

Issues with activities or expenditure

If applicable, identify any ineligible activities or expenditure, the basis of ineligibility and any recommended reductions in the grant amount or changes to activities and milestones if the application is funded.

As part of the eligibility assessment Program Management has identified {Insert comments}
{Insert comments}

Primary assessor - Additional comments / Conditions to funding

{Insert comments}

Secondary assessment Score: XX /100

Individual assessment criterion scores:
AC1 XX /40 AC2 XX /25 AC3 XX /25
AC4 XX /10

Score variation comments (if applicable):
{Insert comments}

General comments:
{Insert comments}

Secondary Assessor Name:
{Insert second assessor's name}

ATTACHMENT C

ASSESSMENT SCORING FRAMEWORK

Scoring

This scoring framework provides a guide for developing each application's scores against the Program's Assessment Criteria. Using the table below, scores are to be allocated on a scale of *Strong* to *No Case* for each Assessment Criterion. Choose the score that best matches the applicant's response. Supporting information provided in the Project Plan, evidence of support and letter of support can be taken into account when determining each score for each Assessment Criterion.

Project size, complexity and grant amount sought

When scoring applications, it is important to consider whether the amount of detail provided by the applicant is relative to project size, complexity and the grant amount sought. Applications with larger more complex projects seeking significant grant funding will provide more detailed responses to the Assessment Criterion compared to applications with smaller less complex projects seeking less grant funding.

Strong	**Good**	**Satisfactory**	**Marginal**	**Poor**	**No Case**
Commensurate with the project size, complexity and grant amount sought, the applicant has provided a **strong** response.	Commensurate with the project size, complexity and grant amount sought, the applicant has provided a **good** response.	Commensurate with the project size, complexity and grant amount sought, the applicant has provided a **satisfactory** response	Commensurate with the project size, complexity and grant amount sought, the applicant has provided a **marginal** response.	Commensurate with the project size, complexity and grant amount sought, the applicant has provided a **poor** response.	Commensurate with the project size, complexity and grant amount sought, the applicant has **not provided a response or has provided a very limited response.**
Criterion 1: score range 32-40	Criterion 1: score range 27-31	Criterion 1: score range 21-26	Criterion 1: score range 13-20	Criterion 1: score range 7-12	Criterion 1: score range 0-6
Criterion 2: score range 21-25	Criterion 2: score range 17-20	Criterion 2: score range 13-16	Criterion 2: score range 9-12	Criterion 2: score range 5-8	Criterion 2: score range 0-4
Criterion 3: score range 21-25	Criterion 3: score range 17-20	Criterion 3: score range 13-16	Criterion 3: score range 9-12	Criterion 3: score range 5-8	Criterion 3: score range 0-4
Criterion 4: score range 10	Criterion 4: score range 8-9	Criterion 4: score range 6-7	Criterion 4: score range 4-5	Criterion 4: score range 2-3	Criterion 4: score range 0-1
• A strong case has been made which is highly convincing and credible. • The response demonstrates excellent capability, capacity and experience relevant to, or understanding of, the requirements of the Criterion. • All indicators* are met to a very high standard. Claims are fully substantiated and information is very clear, comprehensive and convincing. • Thorough analysis and/or evidence provided to support claims. • No to minimal weakness have been identified in limited areas.	• A good case has been made which is convincing and credible. • The response demonstrates good capability, capacity and experience relevant to, or understanding of, the requirements of the Criterion. • Most indicators* are met to a very high standard. Claims are well substantiated and information is clear and convincing. • Relevant analysis and/or evidence provided to support claims. • There may be some weaknesses in limited areas.	• A satisfactory case has been made that is generally reliable and relevant. There may be some irrelevant or ambiguous information. • Most indicators* have been met to a reasonable standard. Claims are reasonably well substantiated and information is generally clear, but there is some detail lacking. There may be some irrelevant or ambiguous information. • Analysis and/or evidence is limited but relevant. • There may be some weaknesses in limited areas.	• A marginal case has been made with supporting analysis that is limited and may not be supported by evidence. • Some indicators* have been met to a reasonable standard, while others are inadequately dealt with. • Supporting analysis and/or evidence is minimal and may be vague. • There may be some significant weaknesses identified in the case made.	• A poor case has been made and there is minimal or no supporting analysis. • Indicators* are inadequately dealt with in most areas. Information is limited, unclear, ambiguous and irrelevant. • Supporting analysis and/or evidence is minimal and poor, and there may be concerns over its reliability. • Major weaknesses are identified.	• No case has been made. • Indicators* have not been addressed, or a very limited response has been provided. • Response raises critical concerns, reservations and risks about the application and the project. • Major weaknesses are identified.

* The dot points under the Assessment Criterion.

Application Number	Applicant	Project Title	Grant Amount Sought	Final Score	Basis for Recommendation	Conditions to Funding
CSSIII000008	FIFTH DOMAIN PTY LTD	CYNAPSE: Benchmarking & Growing Australia's Cyber Operations Workforce	$3,000,000	86	It is recommended that the application be endorsed for funding as it was assessed as highly suitable against the merit criteria. The project demonstrated the following: <u>Strengths:</u> • Well thought out plan, with clear evidence of industry issues and how overcoming. • Strong evidence of wide ranging industry support. • Good measurement of project outcomes. <u>Weaknesses:</u> • No information given on income being generated from the platform. • Potentially could give more evidence on plan to connect with regional/remote target market.	A formal arrangement must be in place with all parties prior to execution of the grant agreement.

S 22

Cyber Security Skills Partnership Innovation Fund Round 2

Committee Application Assessment

1. Application details

Application number	CSSIII000008
Applicant organisation name	FIFTH DOMAIN PTY LTD
Grant amount sought	$3,000,000.00
Primary assessor score	85/100
Secondary assessor score	86 /100
Committee member (primary assessor)	S 22

2. Assessment against the assessment criteria

Refer to the ***Assessment Scoring Framework*** for guidance on scoring each criterion. The following table should be used for guidance on the overall rating. Only applications assessed as highly suitable or suitable should be considered to recommend for funding.

Highly Suitable (84 or more)	Overall, the applicant has provided a strong application whereby the assessment criteria has been addressed to a very high standard. The information provided is clear, convincing and comprehensive, and is generally supported by a thorough analysis and evidence.
Suitable (69 to 83)	Overall, the applicant has provided a satisfactory to good application whereby the assessment criteria has been addressed to a satisfactory to good standard. The information provided is clear but lacking detail. The information is generally supported by relevant analysis and evidence.
Not Suitable (68 or less)	Overall, the applicant has provided a marginal to poor application whereby the assessment criteria has not been addressed to a suitable standard. The information and analysis provided to address the assessment criteria may be clear in some areas but is generally limited, inadequate, unclear or irrelevant.

3. Primary assessment

3.1 Assessment criterion 1 - How your project will improve the quality and availability of the cyber security workforce in Australia, and how innovative it is.

i Score 34/40

ii Comments

Analyse the applicant's response. Include any gaps in the response, or comment on how well the applicant has validated its claims. The applicant was required to demonstrate they meet this criterion by identifying:

- how the project will increase the quality and availability of job-ready cyber security professionals in Australia, including measures that increases the diversity of the cyber security profession, for example women, Indigenous Australians, regional and remote based workers, and neuro diverse individuals. With a focus on how the project will achieve and demonstrate this change
- how the project will help develop the cyber security workforce and meet industry needs
- the extent that the project approach is innovative (new or significantly improved – see the Glossary in the Program Opportunity Guidelines for more information).

Further information: Where relevant applicants should include evidence to support their claims against the criteria, applications with a strong evidence base will be considered more meritorious.

A strong response with strong evidence provided of wide ranging support from industry and stakeholders. all indicators have been addressed, and clear understanding of how the project will increase diversity of cyber security profession. Evidence of industry need for project and innovative design of the project

3.2 Assessment criterion 2 – How the delivery of your project promotes collaboration between industry and the education sector.

i Score 23/25

ii Comments

Analyse the applicant's response. Include any gaps in the response, or comment on how well the applicant has validated its claims. The applicant was required to demonstrate they meet this criterion by identifying:

- the approach/methods it will use to improve collaboration between industry and the education sector
- who the key stakeholders will be and how they propose to work with each of them
- how partnerships formed to deliver your project will have a lasting impact beyond the term of grant funding

Strong case has been made supported by letters of support that include additional tailored comments of support and indicate the value of the project. Clear evidence provided on how the project will engage with industry and project will make lasting impact to overcome current industry problem of being able to assess potential candidates.

3.3 Assessment criterion 3 – Capacity, capability and resources to deliver the project.

i Score 20/25

ii Comments

Analyse the applicant's response. Include any gaps in the response, or comment on how well the applicant has validated its claims. The applicant was required to demonstrate they meet this criterion by identifying:

- their track record managing similar projects and access to personnel with the right skills and experience, including management and technical staff
- their plan to manage the project, addressing scope, implementation plan, timeframes, budget and risk (including any national security risk)
- how they will measure and evaluate the success of the project
- their strategy to maintain the project outcomes beyond the term of the grant funding.

A good case was provided, particularly strong in regards evidence of successfully managing similar projects and personnel that will work on the project.
Good KPIs, but have to assume they will include diversity results
Good project plan, potentially could provide more detail on implementation given size of the project. Also would be interested in further detail on icome generated from platform to determine ongoing viability.

3.4 Assessment criterion 4 – Impact of the grant funding on the project.

i Score 8/10

ii Comments

Analyse the applicant's response. Include any gaps in the response, or comment on how well the applicant has validated its claims. The applicant was required to demonstrate they meet this criterion by identifying:

- how the funding amount requested can be justified with respect to the scale of the project and intended outcomes
- the likelihood that the project would not proceed without the grant. How the grant will positively impact the project, for instance in terms of size, scale and timing
- any additional investment the grant will leverage and explain how this benefits the project.

Good explanation provided on why applying for the grant and the impact it will have on the project is successful (or not). Data gathered from the project will be made widely available to industry and education sector and successful grant will priorities project and enable speed to market to address problem.

3.5 Strengths and weakness of the application

Please note that feedback provided in this section will be passed on to applicants. The information must be presented in clear, concise, and complete sentences that cannot be misconstrued.

Strengths
- Well thought out plan, with clear evidence of industry issues and how overcoming
- Strong evidence of wide ranging industry support
- Good measurement of project outcomes

Weaknesses
- No information given on income being generated from the platform

- Potentially could give more evidence on plan to connect with regional/remote target market
- {Insert weakness}

4. Other considerations

4.1 Issues with activities or expenditure

If applicable, identify any ineligible activities or expenditure, the basis of ineligibility and any recommended reductions in the grant amount or changes to activities and milestones if the application is funded.

As part of the eligibility assessment Program Management has identified {Insert comments} {Insert comments}

4.2 Primary assessor - Additional comments / Conditions to funding

Would be good to understand income generated from platform being created with project and ensure outcome measurements cover diversity data as well.

5. Secondary assessment Score: 86 /100

Individual assessment criterion scores:

AC1	35 /40	AC2	22 /25	AC3	20 /25	AC4	9 /10

Score variation comments (if applicable):
Agree with primary assessment; strong application that looks able to deliver what they have projected with great collaboration that are evidenced to better support the cyber industry broadly. Willing to share data and outcomes which will be valuable to industry collectively in shaping its future.

General comments:
Agree that the platform fills a needed gap in assessment and suitability for industry purposes; could strengthen how this platform will be accessed by whom and at what costs so we can substantiated its ongoing variability either as a business or Industry led tool.

Secondary Assessor Name:
S 22 , NT Regional Manager AusIndustry M) S 22

Australian Government
Department of Industry, Science, Energy and Resources

Commonwealth Standard Grant Agreement

between the Commonwealth represented by

Department of Industry, Science, Energy and Resources

and

FIFTH DOMAIN PTY LTD

Contents

Grant Agreement CSSIII000008

Once completed, this document, together with the Grant Details and the Commonwealth Standard Grant Conditions (Schedule 1), forms an Agreement between the Commonwealth and the Grantee.

Parties to this Agreement

The Grantee

Full legal name of Grantee	FIFTH DOMAIN PTY LTD
Legal entity type (e.g. individual, incorporated association, company, partnership, etc)	Australian Private Company
Trading or business name	FifthDomain
Any relevant licence, registration or provider number	Not applicable
Australian Business Number (ABN) or other entity identifiers	92606251585
Australian Company Number (ACN)	Not applicable
Registered for Goods and Services Tax (GST)?	Yes
Date from which GST registration was effective?	13/07/2015
Registered office address	216 NORTHBOURNE AV BRADDON ACT 2612 Australia
Relevant business place	216 Northbourne Avenue Braddon ACT 2612 Australia

The Commonwealth

The Commonwealth of Australia represented by the
Department of Industry, Science, Energy and Resources
of 10 Binara Street CANBERRA ACT 2600
ABN 74 599 608 295

Background

The Commonwealth has agreed to enter this Agreement under which the Commonwealth will provide the Grantee with a Grant for the purpose of assisting the Grantee to undertake the associated Activity.

The Grantee agrees to use the Grant and undertake the Activity in accordance with this Agreement and the relevant Grant Details.

Scope of this Agreement

This Agreement comprises:

(a) this document;

(b) the Supplementary Terms (if any);

(c) the Standard Grant Conditions (Schedule 1);

(d) the Grant Details;

(e) any other document referenced or incorporated in the Grant Details.

If there is any ambiguity or inconsistency between the documents comprising this Agreement in relation to a Grant, the document appearing higher in the list will have precedence to the extent of the ambiguity or inconsistency.

This Agreement represents the Parties' entire agreement in relation to the Grant provided under it and the relevant Activity and supersedes all prior representations, communications, agreements, statements and understandings, whether oral or in writing.

Certain information contained in or provided under this Agreement may be used for public reporting purposes.

Grant Details CSSIII000008

A. Purpose of the Grant

The Grant is being provided as part of the Cyber Security Skills Partnership Innovation Fund Round 2 grant opportunity.

The objectives of the Cyber Security Skills Partnership Innovation Fund are to:
• increase diversity in the cyber security workforce
• the creation of new and innovative ways to improve the quality and quantity of cyber security professionals in Australia
• improve collaboration between industry and the academia to attract, train and place cyber security talents into their businesses.

The intended outcomes of the Cyber Security Skills Partnership Innovation Fund are:
• increased diversity of the cyber security workforce including lifting the participation of women, Indigenous Australians, regional and remote based workers, and neuro diverse individuals
• delivering a pipeline of highly skilled cyber security professionals to meet with the current and future need of Australia's digital economy
• enhanced Australia's sovereign cyber security capability to underpin our growing digital economy and the safety of all Australians.

B. Activity

The Activity is made up of the Grantee's project and all eligible project activities as specified in these Grant Details.

Project title

CYNAPSE: Benchmarking & Growing Australia's Cyber Operations Workforce

Project scope and description

The scope of the CYNAPSE project consists of 3 streams: 1) Technology platform, 2) Content & analytics & 3) Business Model Generation.

1) Technology platform.
The CYNAPSE technology platform will deliver online & on-demand, hands-on practical SOC assessments for up to 10,000 concurrent users. As this is an integration of technologies (rather than a ground-up build) 6-months is sufficient time to complete these key activities.

Partner Roles.
FifthDomain: Stream Lead. Extend & modify its Labs & Assessor products to facilitate candidate & employer interactions.
s 47G Software service provider. Ensure that honeypot & attack simulation technologies can produce unique assessments
s 47G Software provider. Modify & integrate its cyber case management technology that it is fit-for-purpose for candidates to log their actions in a format which FifthDomain can incorporate into performance analytics.
s 47G Cloud hosting provider. Provide the cloud infrastructure & security monitoring for FifthDomain, s 47G & s 47G technologies to meet scale, security, & availability needs.

Key Activities: FifthDomain will lead the CYNAPSE platform technology integration. This includes: Gather requirements from system users, candidates & employers. Gather requirements from technology partners. Design & validate integration & operation systems with stakeholders. Coordinate the development of the core component modifications & supporting integration technology. Testing & verification of CYNAPSE functional & performance requirements. Deliverables include: Online assessments platform capable of supporting 10,000 concurrent users.

2) Content & Analytics.
CYNAPSE assessments & analytics will prepare candidates for working in a SOC, & provide SOC employers with the insights needed for improved recruitment. 15 assessments will cover five work roles, & three complexity levels. Each assessment will be preceded by one guided formative assessment, & one semi-guided formative assessment, totalling 45 'assessment modules'.

Partner Roles.
FifthDomain: Stream lead. Ensure that SOC employers requirements for assessments & performance insights are collected & validated. Design & develop assessment performance analytics & integrate them into the CYNAPSE platform.
s 47G Assessment designers. Design scenarios for all assessment types & provide the instructional materials for guided & semi-guided formative assessments.
s 47G Assessment simulation developers. Construct the assessment environments based on
s 47G designs.

Key Activities: FifthDomain will lead the Content & Analytics stream, working with candidate supplier & employer stakeholders to design fit-for-purpose assessments & analytics. An assessment design approach will be used for the assessments. Insights will be designed using an Agile methodology.

Key activities: Gather content & analytics requirements from SOC employers. Produce content & analytics designs & validate with SOC employers. Build assessment content materials. Build & integrate assessment environments. Develop analytics data collectors, queries & visualisations. Integrate insights analytics into the platform. Functional & user acceptance testing of assessments content & insights.

Deliverables: 45 online assessment modules within the CYNAPSE platform. 10 performance insights for recruitment decision making.

3) Business Model Generation. The CYNAPSE project will establish a viable business model to connect candidates & employers/recruiters. The model will be sympathetic to the freedoms & constraints of individuals & organisations. It will encompass a fee/compensation model that is attractive & sustainable to maintain CYNAPSE as a commercial business offering.

Partner Role:
FifthDomain: ensure that the commercial model incorporates the interests of candidate & employer stakeholders.
Tech & content suppliers (s 47G): provide multi-year supply agreements. Recruiters & Employers (s 47G): contribute information to establish CYNAPSE usage fee model.
Advocacy partner (s 47G): provide accurate market research information & promotion of CYNAPSE to potential candidates & employers.

Key Activities: As FifthDomain will own the CYNAPSE capability post-project, it will be the lead in developing & establishing the supplier & customer agreements for long-term viability.

Key activities include: Negotiate multi-year supply agreements with technology & content providers. Develop a model for the fixed & variable costs for sustained operation of the CYNAPSE platform. Conduct research into candidate, recruiter & employer desired price points & models for CYNAPSE usage. Develop the CYNAPSE financial model & ongoing business plan. Marketing & promotion of CYNAPSE to the wider market.

Deliverables: Financial model for sustained operation. Business plan for growth

Project outcomes

Outcome 1) An increase in the number of people with assessed cyber skills, & increase in cyber skill proficiency

CYNAPSE is an assessments platform that will 'broaden the funnel' on the talent pipeline & provide users feedback on their performance & recommended resources to improve their performance. The CYNAPSE project aims to promote & make these assessments accessible to candidates beyond those currently working or studying cyber security. Thus, the project outcome will be to increase the number of people with any assessed cyber skills. Given the number and size of project partners, we anticipate the number of candidates that will gain an uplift in skills to be in the thousands, and the number of job placements to be around one hundred. Additionally, the assessments & feedback will compel candidates to conduct further self-education & practice to improve their performance. Thus, leading to an increase in proficiency of those learning cyber security.

Outcome measures:
a) Number of candidates who complete the assessments
b) Number of candidates new to cyber
c) Candidate's perceived increase in skills
d) Number of candidates who have transitioned careers

Outcome 2) Faster & better recruitment of the SOC workforce

Accessing & assessing SOC candidates is difficult for employers & recruiters. Anecdotally, the cost of a bad hire is approximately 3-months salary. Mis-aligned expectations of job duties & required skills is a contributor to those entering the SOC workforce, leaving prematurely. CYNAPSE aims to fix this disconnect between perceived skill needs & actual skill needs by a) providing candidates scenarios they could encounter in the SOC workplace, & b) viewing their own skills in the context of other candidates, which also benefits employers & recruiters with hiring decisions. Access to this pool of candidates & their associated skills metrics will help employers & recruiters make better hiring decisions, faster. Outcomes will be measured through collecting industry baselines for the following metrics & then comparing surveying employer & recruiter partner's experience using the CYNAPSE platform.

Outcome measures:

a) Reduction in time from open position to fulfilment

b) Reduction in unfilled positions
c) Reduction in rehires
d) Increased ability to make more informed hiring decisions; increase in visibility of candidates skills
e) Increased overall effectiveness in aiding organisations to recruit for cyber roles

Outcome 3) Increase diversity of the cyber workforce through advocacy group partnerships & anonymised cyber performance profiles.

Complex cyber operations problems are best solved leveraging the skills, experiences, & perspectives of a diverse SOC workforce. Often the cyber workforce is branded with the 'hooded hacker' stereotype that can a) attract the wrong people, or b) discourage the right people not attracted to cyber. Additionally, unconscious bias may influence employer hiring decisions based on their preconceptions of what makes a 'good' SOC operator, preventing candidates outside this stereotype of 'good' gaining entry into the cyber workforce.

Consequently, the CYNAPSE platform will aim to provide people from remote & diverse backgrounds, & those mid-career looking to transition into cyber, an accessible & safe entry point into the cyber workforce. Candidates demographic information will not be immediately visible to recruiters & employers, only their performance data. This data will not only include their technical abilities but also measures of tenancy, adaptability, & creative problem solving ability.

Additionally, COVID has widened the gap between the digital literate & others. Access to technology is difficult for people in remote areas. This project will work with the Regional University Centres to provide access to the CYNAPSE platform.

Outcome measures:
a) Diverse-background candidate recruitment rates higher than industry benchmarks (where a baseline is available. If no reliable baseline is available, the numbers of candidates for the diversity group will be reported)
b) Number of candidates living in Regional Australia zones (RA2-5)
c) Candidate perception of reduction in bias and ability to showcase skills

Outcome 4) Increase the accuracy & efficiency in the monitoring & evaluation of other training technical cyber programs in producing job ready SOC operators.

Significant Federal & State Government investment is being made in cyber education & training programs. Monitoring & evaluation of these programs is required not only to demonstrate responsible use of public money, but also to understand if Australia is taking the best approach to protecting its national cyber security interests. The CYNAPSE project provides two important data points for evaluation of existing training & education programs in producing the cyber operations workforce: 1 - the education & training backgrounds of the highest performing candidates & 2 - the education & background of the highest recruited & retained candidates. CYNAPSE will be available to assess suitable graduates from other relevant CSSPIF programs, including but not limited to the s 47G led s 47G project (of which FifthDomain is a partner).

Outcome measures:
a) Effectiveness & utility of CYNAPSE insights to stakeholders involved with monitoring & evaluating cyber education & training programs.

In undertaking the Activity, the Grantee must comply with the requirements of the grant opportunity guidelines (as in force at the time of application).

The Grantee must notify the Commonwealth about events relating to the project and provide an opportunity for the Minister or their representative to attend.

C. Duration of the Grant

The Activity starts on 15 December 2022 and ends on 14 December 2024, which is the **Activity Completion Date**.

The Agreement ends on 23 May 2025 which is the **Agreement End Date**.

Activity Schedule

In undertaking the Activity, the Grantee will meet the following milestones by the due dates.

Milestone number	Milestone name and description	Due date
001	Milestone 1 - Project initiation Outcome: The project team, governance, processes, & commercial agreements are established. -Establish commercial agreements between project partners -Establish financial management practices between project partners -Establish grant agreement between FD & Commonwealth -Establishing project governance committees & communications -Establish information management policies & procedures -Establishing roles & responsibilities for delivery -Recruitment & onboarding of staff / contractors Deliverables: -Commonwealth Agreement -Communications & Reporting Schedule -Detailed project plan	30/03/2023

Milestone number	Milestone name and description	Due date
002	Milestone 2 - Design & development Outcome: CYNAPSE platform is ready to be piloted. Build Assessment Content Gather industry requirements Develop formative assessments Develop dynamic summative assessments Test assessment content material Build Assessment Insights Gather industry requirements for performance insights Design & Develop analytics for performance insights Functionally test data collection & analytics Gather & implement user feedback on assessment insights Build & Integrate Platform Technology Gather functional requirements Gather non-functional requirements Design platform system Develop & integrate technology components Test & transition platform into production Deliverables: CYNAPSE platform 45 Assessments 10 Performance Analytics	30/09/2023
003	Milestone 3 - Pilot & refine Outcome: CYNAPSE platform is improved based on the feedback from users & employers from the pilot & ready for public usage. -Design pilot scope, objectives, & user cohort composition -Gather users for pilot cohort -Provide instruction & onboarding to pilot cohort -Support pilot cohort conduct of assessments -Collect, analyse, & report pilot cohort feedback -Provide user cohort performance reporting to suitable employer/recruiter partners -Integrate employer/recruiter & user feedback into platform improvements work Deliverables: -Pilot feedback report -Anonymised user performance report	30/03/2024

Milestone number	Milestone name and description	Due date
004	Milestone 4 - Assess & recruit Outcome: The CYNAPSE platform is proven to generate desired outcomes for candidates, recruiters, & employers. -Market & promote the CYNAPSE program through partner & public channels -Provide instruction & onboarding to users -Market CYNAPSE to wider employers & recruiters -Collect, report, & integrate rolling feedback -Monitor & manage employer to candidate interactions -Report on candidate number, usage, employer connections, & hires -Build commercial model for candidates , recruiters, & employers -Establish contractual agreements with technology suppliers -Establish contractual agreements with employers & recruiters Deliverables: -Report - candidate numbers, employer connections, hires.	30/11/2024
005	Milestone 5 - Project close & Transition to BAU Outcome: CYNAPSE establishes the necessary commercial agreements for continued operation beyond the project. -Post-project administration & reporting Deliverables: -Project reporting	14/12/2024

S 22

S 22

S 22

S 22

Supplementary Terms

S 22

S 22

S 22

S 22

S 22

S 22

S 22

S 22

S 22

Schedule 1: Commonwealth Standard Grant Conditions

S 22

S 22

S 22

S 22

S 22

S 22

S 22

S 22

S 22

S 22

Schedule 2 Reporting requirements

Appendix 1

Cyber Security Skills Partnership Innovation Fund Round 2 - progress report requirements

You will need to provide the following information in your progress reports. The Commonwealth reserves the right to amend or adjust the requirements.

You must complete and submit your report on the portal. You can enter the required information in stages and submit when it is complete.

Project progress

a. Complete the following table, updating for all milestones shown in the Activity Schedule of your grant agreement.

Milestone	Agreed end date	Actual/ anticipated end date	Current % complete	Progress comments – work undertaken and impact of any delay

b. Where applicable, describe any project activities completed during the reporting period that are not captured in the table above.

c. Is the overall project proceeding in line with your grant agreement?

If no, identify any changes or anticipated issues. Comment on any impacts on project timing and outcomes and how you expect to manage these.

d. Are there any planned events relating to the project that you are required to notify us about in accordance with your agreement?

If yes, provide details of the event including date, time, purpose of the event and key stakeholders expected to attend.

Project outcomes

a. Outline the project outcomes achieved to date.

b. Have you created an innovative solution to improving the quality, quantity or diversity of job-ready cyber security professionals in the reporting period? If yes describe.

c. Have you created any additional partnerships/collaborations to support your project in the reporting period? If yes describe.

Project expenditure

Provide the following information about your eligible project expenditure. Eligible expenditure is divided into the same categories as the budget in your application.

If you are registered for GST, enter the GST exclusive amount. If you are not registered for GST, enter the GST inclusive amount. We may ask you to provide evidence of costs incurred.

Refer to the grant opportunity guidelines or contact us if you have any questions about eligible expenditure.

a. What is the eligible expenditure you have incurred in this reporting period?

b. What is the estimated eligible expenditure for the next reporting period?

c. What is the estimated eligible expenditure for remaining reporting periods in current financial year (if applicable)?

d. What is the estimated total eligible expenditure for future financial years?

e. What is the estimated total eligible expenditure for the project?

f. Briefly explain the reason for any changes between the forecast and actual expenditure for the current reporting period, and any significant changes to the forecast budget for the remainder of the project.

g. Is the project expenditure broadly in line with the activity budget in the grant agreement?

If no, explain the reasons.

Project funding

a. Provide details of all contributions to your project other than the grant. This includes your own contributions as well as any contributions from project partners or others.

Attachments

a. Attach any agreed evidence required with this report to demonstrate project progress.

b. Attach copies of any published reports and promotional material, relating to the project.

Certification

You must ensure an authorised person completes the report and can declare the following:

- The information in this report is accurate, complete and not misleading and that I understand the giving of false or misleading information is a serious offence under the *Criminal Code 1995* (Cth).
- The activities identified in this report are for the purposes stated in the grant agreement.
- I am aware of the grantee's obligations under their grant agreement, including the need to keep the Commonwealth informed of any circumstances that may impact on the objectives, completion and/or outcomes of the agreed project.
- I am aware that the grant agreement empowers the Commonwealth to terminate the grant agreement and to request repayment of funds paid to the grantee where the grantee is in breach of the grant agreement.

Appendix 2

Cyber Security Skills Partnership Innovation Fund Round 2 - end of project report requirements

You will need to provide the following information in your progress reports. The Commonwealth reserves the right to amend or adjust the requirements.

You must complete and submit your report on the portal. You can enter the required information in stages and submit when it is complete.

Project achievements

a. Complete the following table, updating for all milestones shown in the Activity Schedule of your grant agreement.

Milestone	Agreed end date	Actual/ anticipated end date	Current % complete	Progress comments – work undertaken and impact of any delay

b. Where applicable, describe any project activities completed during the reporting period that are not captured in the table above.

c. Have you seen an increase in the ***number*** of job-ready cyber security professionals as a result of your project? If yes, how many?

d. Will your project continue to increase the ***number*** of job-ready cyber security professionals? If yes, how many? Over what period?

e. Have you seen an increase in the ***quality*** of cyber security professionals as a result of your project? If yes describe.

f. Will your project continue to increase the ***quality*** of cyber security professionals? If yes describe.

g. Have you seen an increase in *workforce diversity (demographics) in the cyber security profession* as a result of your project? If yes, what diverse cohorts? How many?

h. Will your project continue to increase the workforce diversity *in the cyber security profession*? If yes, by how many? Over what period?

i. Did your project produce an innovative solution to improving a cyber security problem? If yes describe.

j. Did your project create any innovative and/or new ways of reskilling or upskilling people to join the cyber security workforce? If yes describe.

k. Identify from the list below which categories best describe your innovative/ new approach/s.

- specialist cyber security courses
- retraining (upskilling or reskilling)
- cyber labs, training facilities, cyber simulators
- professional development for teachers
- professional development for board executives
- student delivered cyber security services
- scholarship, internship, cadetship, apprenticeship programs
- work experience or staff exchange programs
- Other (describe)

l. How did your project meet cyber security industry needs not met by other education services?

Project outcomes

a. Outline the project outcomes achieved by the project end date.

b. Do the achieved project outcomes align with those specified in the grant agreement?

If no, explain why.

c. Are there any planned events relating to the project that you are required to notify us about in accordance with your agreement?

If yes, provide details of the event including date, time, purpose of the event and key stakeholders expected to attend.

d. Have you created any additional partnerships/collaborations to support your project? If yes describe.

e. Identify from the list below, the types of organisation that best describe your project partners/ collaborators?

- Industry
- Government
- Businesses
- Schools and tertiary education providers

f. Will the partnerships/collaborations you have developed continue beyond the duration of this grant opportunity? If yes describe.

g. If your project is focussed on a particular geographical area or a specific cohort, could it be scaled up or translated to another geographical area or different cohort? If yes, describe how.

h. Reflecting on the overall project, what are the two or three key learnings that could inform the design and conduct of similar projects in the future?

i. Are there any planned events relating to the project that you are required to notify us about in accordance with your agreement?

If yes, provide details of the event including date, time, purpose of the event and key stakeholders expected to attend.

Project benefits

a. What benefits has the project achieved?

b. What ongoing impact will the project have?

c. Did the project result in any unexpected benefits or unplanned negative outcomes?

If yes, explain what these were and why.

d. Is there any other information you wish to provide about your project?

If yes, provide details.

Total eligible project expenditure

a. Indicate the total eligible project expenditure incurred. Eligible expenditure is divided into the same categories as the budget in your application.

If you are registered for GST, enter the GST exclusive amount. If you are not registered for GST, enter the GST inclusive amount. We may ask you to provide evidence of costs incurred.

Refer to the grant opportunity guidelines or contact us if you have any questions about eligible expenditure.

b. Provide any comments you may have to clarify any figures.

c. Was the expenditure incurred in accordance with the activity budget in the grant agreement?

If no, explain the reason for a project underspend or overspend, or any other significant changes to the budget.

Project funding

a. Provide details of all contributions to your project other than the grant. This includes your own contributions as well as any contributions from project partners or others.

Attachments

a. Attach any agreed evidence required with this report to demonstrate progress or successful completion of your project.

b. Attach copies of any published reports and promotional material, relating to the project.

Certification

You must ensure an authorised person completes the report and can declare the following:

- The information in this report is accurate, complete and not misleading and that I understand the giving of false or misleading information is a serious offence under the *Criminal Code 1995* (Cth).
- The grant was spent in accordance with the grant agreement.
- I am aware of the grantee's obligations under their grant agreement, including survival clauses.

- I am aware that the grant agreement empowers the Commonwealth to terminate the grant agreement and to request repayment of funds paid to the grantee where the grantee is in breach of the grant agreement.

S 22

S 22

S 22

S 22

S 22

S 22

S 22

S 22

S 22

S 22

S 22

S 22

KPMG

Evaluation of the Cyber Security Skills Partnership Innovation Fund

Final Report

Department of Industry, Science and Resources

29 July 2022

KPMG.com.au

KPMG

Disclaimer

Inherent Limitations

This Evaluation Report (the Deliverable) has been prepared as outlined with the Department of Industry, Science and Resources (the Department) in the Scope Section of the engagement Work Order (SON3352211; CON005101). The services provided in connection with this engagement comprise an advisory engagement, which is not subject to assurance or other standards issued by the Australian Auditing and Assurance Standards Board and, consequently no opinions or conclusions intended to convey assurance have been expressed.

The findings in this Deliverable are based on a qualitative study and the reported results reflect a perception of the Cyber Security Skills Partnership Innovation Fund but only to the extent of the sample surveyed, being the Department's approved representative sample of stakeholders. Any projection to the wider stakeholder base is subject to the level of bias in the method of sample selection.

No warranty of completeness, accuracy or reliability is given in relation to the statements and representations made by, and the information and documentation provided by, the Department's management, and personnel and stakeholders consulted as part of the process.

No reliance should be placed by the Department on additional oral remarks provided during any presentation of this Deliverable, unless these are confirmed in writing by KPMG.

KPMG have indicated within this Deliverable the sources of the information provided. We have not sought to independently verify those sources unless otherwise noted within the report.

KPMG is under no obligation in any circumstance to update this Deliverable, in either oral or written form, for events occurring after this Deliverable has been issued in final form.

Third Party Reliance

This Deliverable is solely for the purpose set out in the Scope Section and for the Department's information, and is not to be used for any purpose not contemplated in the engagement Work Order or to be distributed to any third party without KPMG's prior written consent.

This Deliverable has been prepared at the request of the Department in accordance with the terms of KPMG's engagement letter/contract dated 08 April 2022. Other than our responsibility to the Department, neither KPMG nor any member or employee of KPMG undertakes responsibility arising in any way from reliance placed by a third party on this Deliverable. Any reliance placed is that party's sole responsibility.

Document classification: KPMG Confidential.

1 Contents

List of attachments

Attachment A. Cyber Security Industry – Workforce Pipeline Survey Results

Attachment B. Cyber Security Skills Partnership Innovation Fund (CSSPIF) Survey Results

Attachment C. Data matrices of CSSPIF applications' attributes

Attachment D. Whiteboard from Cyber Security Workforce Growth Programs Workshop (high resolution)

List of tables

List of figures

Glossary

Table 1: Glossary of terms used in this report

Term	Definition
ACSC	Australian Cyber Security Centre
ADII	Australian Digital Inclusion Index
AI	Artificial Intelligence
AI/ML	Artificial Intelligence / Machine Learning
AICD	Australian Institute of Company Directors
AIIA	Australian Information Industry Association
ASD	Australian Signals Directorate
ASIA	Australian Information Security Association
AQF	Australian Qualifications Framework
BCP	Cyber Security Business Connect and Protect program
CEO	Chief Executive Officer
CI	Critical Infrastructure
CSAT	Cyber Security Assessment Tool
Cyber CRC	Cyber Security Cooperative Research Centre
CSSPIF	Cyber Security Skills Partnership Innovation Fund
DFAT	Department of Foreign Affairs and Trade
DISR	Department of Industry, Science and Resources
DSO	Digital Skills Organisation
ICT	Information and Communications Technology
IT	Information technology
KEQ	Key Evaluation Question
NCSC	National Cyber Security Centre
NDIS	National Disability Insurance Scheme
NICE	National Initiative for Cybersecurity Education
NGO	Non-government organisations
NSC	National Security College
OT	Operational Technology
RMIT	Royal Melbourne Institute of Technology
RTO	Registered training organisation
SME	Small-to-medium-sized enterprise
STEM	Science, technology, engineering and mathematics
VET	Vocational Education and Training

2 Executive summary

2.1 Program and evaluation purpose

A strong cyber security workforce is a key enabler to growing Australia's digital economy and protecting individuals and the nation from malicious cyber activity. However, there is a gap between the demand for, and supply of, suitably skilled cyber security professionals. As the pace of technological change accelerates and Australia becomes even more reliant on the digital ecosystem for both prosperity and security, this gap will grow in the absence of effective action.

The Cyber Security Skills Partnership Innovation Fund (CSSPIF) was established in 2020 to improve the quality and quantity of cyber security professionals in Australia, and to strengthen partnerships and collaboration between industry and academia. In total, the Australian Government has made $70.3M available to CSSPIF over four years from 2020-2024 to fund innovative local projects delivered in partnership with industry, academia, and government. So far, eight projects have been funded (Round 1); and another 18 projects are expected to be funded in FY22-23 (Round 2 - pending announcement).

Two years after the commencement of the Program, the Department of Industry, Science and Resources (DISR) has commissioned this interim evaluation of the CSSPIF. The evaluation has considered five key evaluation questions (KEQ) organised into four themes of inquiry: program design (KEQ 1-2); program delivery and implementation (KEQ 3-5); early outcomes of the Program overall (individual project outcomes not in scope); and lessons learned from the Program to date and potential for improvement. **Appendices A** and **B** outline the methodology and extensive engagement underpinning the evaluation.

2.2 Evaluation Findings

2.2.1 Program design

KEQ 1. To what extent does the CSSPIF's design meet the Government's strategic interest in growing a robust and secure digital economy?

Overall, the CSSPIF Program Design is suitable, but there is room for improvement to address unmet needs of some key stakeholder groups. This evaluation found that the Program's design broadly meets the Australian Government's strategic interests in this area. It does so by supporting the growth of the cyber security workforce through a wide range of approaches, including efforts to increase the participation of underrepresented cohorts in the workforce. There is an opportunity for the CSSPIF to be more focused in targeting specific areas of industry need, rather than providing a broad approach.

KEQ 2. How well do the CSSPIF grant opportunity guidelines match the industry's interest in, and capability to, meet the requirements?

The evaluation found that the CSSPIF grant opportunity guidelines match industry interest in, but not all of the industry's capability to, meet the requirements. It was observed that the Program's design suits a target audience of bigger, better resourced and more experienced applicants. Some interviewees believed program eligibility conditions that suit larger, more experienced applicants were unlikely to result in projects that shift the dial in the cyber skills pipeline. Barriers to participation such as the 50 per cent co-contribution (at a minimum of $250,000) limit the pool of potential applicants. This is particularly pertinent as firms in the cyber security sector are mostly 'young' (i.e. founded within the past decade) and small (i.e. fewer than 100 employees).

2.2.2 Program delivery and implementation (KEQ 3-5)

KEQ 3. How well did the Program reach and engage with the intended stakeholders for CSSPIF Rounds 1 and 2?

This evaluation found that the Program has been moderately effective at reaching and engaging the intended stakeholders. It was observed that internal management of communications needed clearer expectations; external promotion needed planning and input from target audiences to be more effective, and a greater understanding of who the intended audience is; and program communication activities post-funding rounds have been limited to date.

KEQ 4. How effectively was the Program delivered?

This evaluation found that the Program has been effectively delivered in the context of being a new program established during COVID-19 lockdowns. Program promotion and communication was adequate but can be improved to increase awareness and visibility of grant recipient projects. Risks for assessment and funding activities were managed effectively. While there appears to have been a difference in risk appetite between Round 1 and Round 2, the additional funding allocated to the Program between rounds provides a rationale for this pragmatic approach. An opportunity exists to maintain contact with the pool of applicants rated as 'suitable but not funded' to encourage them to apply for any future funding rounds, noting that 18 such applicants from Round 1 did not re-apply.

KEQ 5. To what extent did broader environmental factors impact performance or quantity and quality of the Program's subscription?

This evaluation found that the environmental factors appear to have had minimal short-term impact in disrupting program implementation, but project roll-out has been delayed. It was observed that while the COVID-19 pandemic has likely affected some potential applicants, it has not materially deterred growth in industry co-investment. Beyond the COVID-19 pandemic, the skills shortage itself, the complicated digital and cyber environment where both Government and industry are vying for engagement from key stakeholders, and the wider skills shortage across industries are broader environmental factors at play.

2.2.3 Early outcomes of the Program overall

Key short-term outputs and outcomes of the CSSPIF Program indicate that the Program is on-track to meet its intended objectives. Overall, short-term outputs and outcomes of the CSSPIF Program have been largely positive. It was observed that: CSSPIF projects are encouraging industry co-investment, which has increased between Rounds 1 and 2; CSSPIF projects are increasingly responsive to diversity issues in the cyber security workforce; CSSPIF projects are supporting industry efforts to increase the quality and quantity of cyber security professionals in Australia; and CSSPIF projects are improving collaboration between industry and the education sector.

2.2.4 Lessons learned from the Program to date and potential for improvement

There continues to be a role for Government in addressing the cyber security skills gap, but this must be done together with industry.

The cyber security industry is funding and developing its own workforce initiatives (outside of CSSPIF). However, such initiatives are ad hoc and tend to focus on benefiting their own immediate organisational workforce pipelines, not the sector at large. There is the opportunity for the cyber security industry to collaborate more to address shared problems, like the skills shortage, and for the CSSPIF to contribute to this goal. Government can play a convening role to facilitate this.

Government also has a key role in supporting the training and employment pathways of the cyber security industry and providing leadership. Industry representatives see the government's value lies in creating a coordinated policy context and clear signals to the market; co-investment in best practice; and efficient regulation. Industry representatives welcome the support of government collaboration on issues impacting the sector; and see government as a key partner in regulating the quality of the cyber security education and training system.

The evaluation found that the skills shortage affecting the industry at large is constraining the sector's capacity to recruit experienced professionals who can deliver training to the current and future cyber security workforce and grow the talent pipeline needed to manage cyber security risks to our economic and national security. This evaluation found that future programs addressing the cyber security skills shortage and talent pipeline need address this issue of qualified trainer availability.

Sustained growth of the cyber security skills pipeline involves both encouraging and training more people to enter the sector, and also encouraging people to remain in that sector. Beyond competitive salaries, workforce retention is also dependent on making the industry's workplaces psychologically secure, diverse and equitable environments for all employees. This evaluation found that more research into the Australian cyber security industry's diversity and workplace environments is needed to inform future policy and programs.

2.3 Summary of recommendations

Industry feedback indicates that there remains a genuine need and interest in the CSSPIF. This report contains 14 key recommendations for the Department's consideration. In summary, recommendations suggest:

- Addressing points of friction in the program design through stakeholder co-design and incorporating lessons learned in the first two rounds.
- Ensuring all internal and external communications foster a joint understanding of what is expected of stakeholders to minimise any potential for misunderstanding.
- Clarifying CSSPIF's place in the cyber skills landscape to identify distinct, priority areas for action.

Table 2. Summary table of CSSPIF evaluation recommendations.

#	Recommendation
	Program Design
1	Key program design features should be retained but lessons learned from funding rounds should be incorporated to ensure alignment with shifting government priorities based on industry need. These activities should: a. Map and analyse other programs across the digital economy to understand specific value-add of CSSPIF in this broader market/system. b. Conduct in-depth market research into who the Program is trying to reach, and market capacity to co-contribute funding to match the volume of available Commonwealth funds. c. Clarify which roles/skills gaps (identified by industry representatives) are to be addressed through future funding rounds. For example, this could involve targeting the higher-priority skills types and novel digital skills, or targeting specific regulatory reforms (e.g. Critical Infrastructure) that require cyber industry workforce support to implement.
2	Co-design future rounds with targeted population segments so the Program can be better informed and promoted to reach and benefit the intended audience. These activities should: a. Identify intended stakeholders to ensure that they are appropriately targeted. b. Co-design the Program's future rounds and any guideline updates with key stakeholder groups to better target the needs of industry and disadvantaged stakeholder groups. This should explore government and industry targets (both realistic and aspirational) in relation to key program outcomes. c. During the development of guidelines, consult with peak bodies and representatives of the underrepresented cohorts that the Program intends benefit.
3	Explore alternative mechanisms to mitigate risk (e.g. partnership arrangements, co-contributions and liquid assets) as a means of supporting participation of start-ups and niche groups who may find it more difficult to access large amounts of capital that would otherwise enable them to meet co-contribution and liquidity requirements. For example, allow for smaller 'quick win' projects that come with smaller co-contributions amounts (i.e. below $50,000).

#	Recommendation
	Program delivery and implementation
4	Develop a detailed communications plan in consultation with key stakeholders to ensure the intended audience is being reached. This should include: a. Ensuring that timing of when guidelines are released, applications are due, and implementation milestones are due, correspond with optimal marketing events (e.g. Cyber Week) and industry needs (e.g. longer timeframes to prepare applications). b. Hosting webinars, with participation from CSSPIF Program alumni, to promote the CSSPIF and engage stakeholders in the content prior to application close dates. c. Setting clear intentions, instructions and sought-after outcomes when reaching out through departmental networks to promote the CSSPIF.
5	Additional clarity around weighting of assessment criteria is needed to ensure the efficient use of resources and support both applicants, assessment committee members and the Department.
6	Clarify forms of acceptable in-kind co-contributions and how to estimate their value.
7	Clarify in the guidelines what is required of applicants to demonstrate how the proposed project will best meet the needs of the intended beneficiary groups.
8	Include representatives from minority or disadvantaged groups in assessment committees to ensure applicants' claims about meeting stakeholder needs are verifiable and appropriate.
	Early outcomes of the Program overall
9	Establish a CSSPIF Program alumni group to support networking, cross-promotion and shared learnings among grant recipient projects.
10	Reporting on the intended program outcomes and setting year-on-year targets to increase diversity, lift the participation of women, Indigenous Australians, remote based worker and neurodiverse individuals to increase accountability and measure program performance.
11	Explore options to track and measure the benefits of the numerous partnerships fostered through this Program.
	Lessons learned from the Program to date and potential for improvement
12	Gather more comprehensive data on the needs and diversity of the cyber security skills pipeline and current workforce.
13	Map and analyse government cyber security workforce initiatives to identify current and emerging priority areas and better coordinate initiatives across government to target gaps and avoid duplication.
14	Stand up an interdepartmental reference group / committee (that also links in with relevant officers from State and Territory Governments) which coordinates policy and programs that serve to grow the cyber security and broader digital workforce.

3 Introduction

This section provides an overview of the CSSPIF Evaluation Report (the "Report") structure along with a brief description of the evaluation background and purpose.

3.1 Structure of this report

This report has been divided into 13 parts (shown in in Table 3) and should be read in conjunction with **Appendices A-F**. Further detail underpinning the evidence provided in Appendices C and D is provided as attachments to this Report (See the list of attachments provided on page 4 of this Report).

Table 3: CSSPIF Evaluation Report Structure

Ch. #	Chapter (Ch.) label	Chapter Contents
1	Contents	Provides index lists of chapters, attachments, tables and figures.
2	Executive summary	Provides an overview of the evaluation scope, approach, observations, and findings which respond to the key evaluation questions.
3	Introduction	Provides background information about the CSSPIF Program and the purpose of this evaluation.
4	Evaluation Approach	Provides and overview of the approach used to guide evaluation activities, including a description of evaluation scope, objectives, methods and limitations.
5	Discussion: Key evaluation questions	A discussion of key findings and relevant observations that respond to the key evaluation questions.
6	Conclusion	Closing reflections on the results and implications of this evaluation.
7	Recommendations	Provides a set of recommended actions for the Department's consideration, with references to relevant observations supporting the recommendation
8	Appendix A – Evaluation method	Provides a detailed description of the method used to conduct evaluation activities.
9	Appendix B – Index of CSSPIF interviews and workshops	Provides a list of all interviews and workshops conducted with stakeholders consulted to inform this evaluation.
10	Appendix C – Observations of the CSSPIF Program Context	Provides contextual observations, including the government and industry's interest in growing the digital economy and addressing the cyber security skills gap.
11	Appendix D – Observations of the CSSPIF Program Logic	Provides observations on the program inputs, design and implementation activities and the initial outputs and outcomes associated with the Program to date in line with the program logic.
12	Appendix E – Cyber Security Workforce Pipeline	Provides graphics that illustrate the distribution of cyber security workforce growth initiatives across the workforce pipeline.
13	Appendix F – CSSPIF partnerships and networks	Provides graphics that illustrate the connections between the partnerships and networks fostered through CSSPIF-funded projects.

3.2 The Cyber Security Skills Partnership Innovation Fund (CSSPIF) Program

The Australian Government's Cyber Strategy 2020 identified that the resilience of Australia's digital economy to cyber security incidents has been challenged in part by workforce constraints (i.e. shortage of suitably skilled people to enact cyber risk prevention measures) and low cyber maturity of individuals and organisations in adopting cyber risk mitigation. In response, funding was announced for programs to address these challenges. Delivered by the Department of Industry, Science and Resources (the Department), the CSSPIF program is activating non-government and private sector efforts to improve Australia's cyber resilience.

The overarching policy intent of the CSSPIF is to increase the pipeline of Australian cyber security professionals. The Australian Government initially announced $26.5M over four years from 2020 – 2024 to fund innovative local projects delivered in partnership with industry, academia, and government under the *Cyber Security Strategy 2020*. This was supplemented in 2021-22 by a $43.8M injection under the *Digital Economy Strategy*, bringing the total funding of the Program to $70.3M over 2020-2024.

Applications for the CSSPIF were required to be joint applications, with a lead applicant that meets the eligibility criteria and at least one other project partner. For Round 1, lead applicants were required to be an entity, associated or not-for-profit organisation incorporated in Australia or state, territory or local government agency or body. In Round 2, state, territory or local government agencies or bodies were no longer allowed to be lead applicants, but could still be a partner in applications. The grant amount is up to 50 per cent of total eligible project expenditure, with the minimum grant of $250,000 and maximum grant of $3 million.

In June 2021, just under a third (31.3 per cent or $8.3M) of the initial funding ($26.5M) was awarded to eight successful projects in Round 1 of the Program. Round 2 of the Program opened for applications in October 2021 with up to $60.1M in funding remaining available. Successful applicants from Round 2 are expected to be announced in FY 2022-23, with the amount recommended to be funded in Round 2 is $25.4M – taking up 42 per cent of the funding remaining available.

The case for an additional Round of the CSSPIF is currently being considered by the Department.

3.3 Purpose of this evaluation

In April 2022 the Department engaged KPMG to conduct an evaluation of the CSSPIF, the Cyber Security Business Connect and Protect program (BCP) and the Cyber Security Assessment Tool (CSAT). The evaluations are being delivered in three separate phases. Phase 1 requires and evaluation of the design and implementation of the two rounds of CSSPIF, including factors that influenced industry participation and opportunities for future directions.

The purpose of the CSSPIF evaluation was to review the design, delivery, and early effectiveness of the Program overall (rather than individual project outcomes) to help inform future policy development aimed at supporting growing the cyber security and digital technology workforce.

4 Evaluation Approach

This section provides an overview of the evaluation approach used to inform the key observations and describes the evaluation scope and objectives, methods and limitations. The detailed evaluation approach is described in **Appendix A** of this report.

4.1 Evaluation scope and objectives

4.1.1 Nature of the evaluation and review

The purpose of the CSSPIF evaluation is to review the design, delivery, and early effectiveness of the Program overall (rather than individual project outcomes) to help inform future policy development aimed at growing the cyber security and digital technology workforce in Australia. The project sought to answer the evaluation questions detailed in section 4.1.2 below, which focus on the **design** and the **implementation** of the CSSPIF. The evaluation approach consisted of the following 3 stages:

- Stage 1: Evaluation planning and design;
- Stage 2: Conducting the evaluation; and
- Stage 3: Reporting.

4.1.2 Key evaluation questions

To explore the CSSPIF, the evaluation considered the following five overarching key evaluation questions and sub-questions:

Program Design

1. **To what extent does the CSSPIF's design meet the Government's strategic interest in growing a robust and secure digital economy?**
   - *Are there specific areas of the cyber industry that the CSSPIF could/should be focussed towards?*
   - *What opportunities exist to expand the scope of the Program to support workforce growth of other digital technology industries (e.g. artificial intelligence (AI) and quantum computing)?*

2. **How well do the CSSPIF grant opportunity guidelines match the industry's interest in, and capability to, meet the requirements?**
   - *What elements (e.g. financial co-contribution, project or eligibility) of the grant opportunity guidelines could be altered to improve its outcomes?*
   - *To what extent did the nature and magnitude of the problem or opportunity that CSSPIF is designed to address change?*
   - *What opportunities exist for the Program to adapt to the shifting market demand for cyber security professionals?*

Program Implementation

3. **How well did the Program reach and engage with the intended stakeholders for CSSPIF Rounds One and Two?**
   - *What are some opportunities for future rounds that could enhance program reach, uptake and more quality applications?*
   - *How could a Round Three be better targeted to meet industry needs?*

4. **How effectively was the Program delivered?**
   - *Was the Program promotion and communication effective?*
   - *How well were risks anticipated, mitigated and managed?*

5. **To what extent did the market, policy, economic environment and timing affect performance or quantity and quality of the Program's subscription?**

4.2 Summary of Evaluation Activities

The evaluation involved in-depth reviews of documentation provided by the Department of Industry, Science and Resources (DISR) and from open sources; and extensive stakeholder consultation. The approach taken is outlined in Figure 1 below.

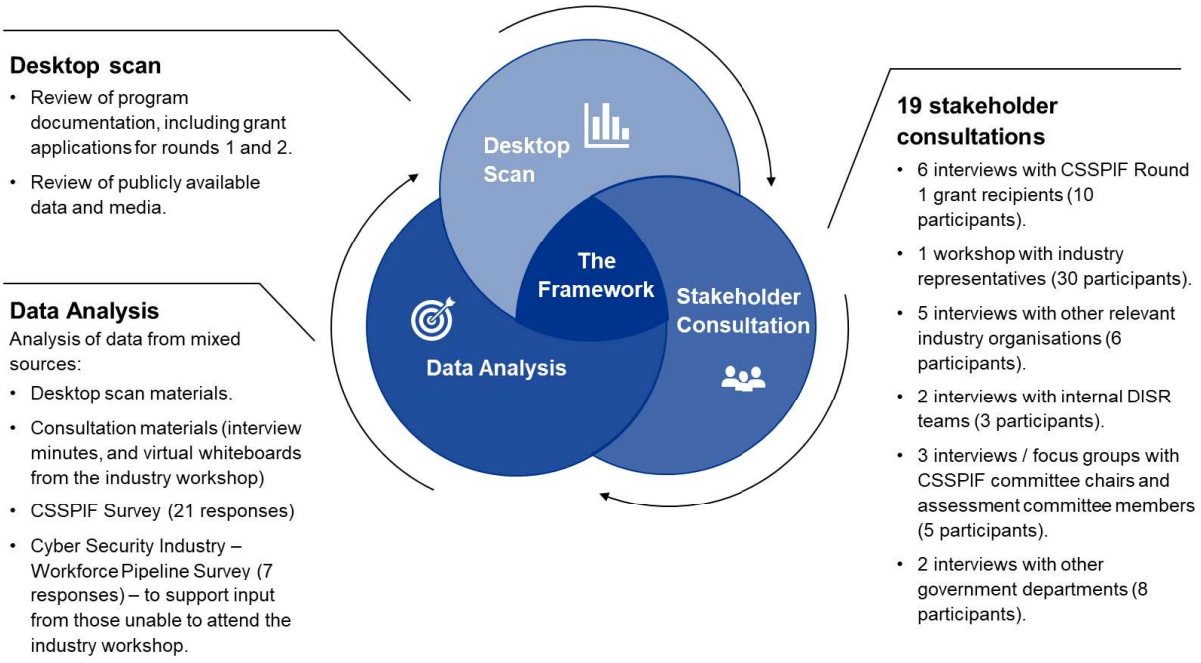


Figure 1: Key evaluation activities.

4.3 Evaluation considerations and limitations

This was a design and implementation evaluation. The projects funded in CSSPIF Round 1 have not concluded, yet; and the successful applicants for Round 2 had not yet been announced. Consequently, there is limited data to assess the outcomes of the Program. The data obtained to inform this evaluation has been sufficient to undertake an evaluation of the design and implementation of the Program.

The following key considerations were identified for the evaluation of the Program:

- The design evaluation focuses on the attributes of the Program, and the alignment of these attributes to the strategic intent of the Program.
- The implementation evaluation focuses on implementation effectiveness and lessons learned; Program reach and take-up; appropriateness of the Program delivery management approach over the life of the Program to date.
- Identification of necessary changes in grant opportunity guidelines and whether there are opportunities to improve the efficiency and effectiveness of the grants process.
- Acknowledging how COVID-19 may have affected funded organisations and their projects.
- Ensuring the work produced from the evaluations produces actionable findings and recommendations to inform further Program development.

Limitations affecting confidence in observations and findings of the evaluation included:

- Data available to explore potential barriers to submitting grant applications.
- Limited access to stakeholders to participate in consultations.
- Limited access to program documentation.

5 Discussion: Key evaluation questions, early outcomes, and lessons learned

This chapter discusses key findings from the evaluation observations of the Program Context (see Appendix C) and the Program Logic (see Appendix D). The evaluation has considered five key evaluation questions (KEQ) organised into four themes of inquiry:

- Program design (KEQ 1-2);
- Program delivery and implementation (KEQ 3-5);
- Early outcomes of the Program overall (individual project outcomes not in scope); and
- Lessons learned from the Program to date and potential for improvement.

5.1 Design

5.1.1 Key Evaluation Question 1 – Strategic Interest

To what extent does the CSSPIF's design meet the Government's strategic interest in growing a robust and secure digital economy?

- Are there specific areas of the cyber industry that the CSSPIF could/should be focussed towards?
- What opportunities exist to expand the scope of the Program to support workforce growth of other digital technology industries (e.g. artificial intelligence (AI) and quantum computing)?

Summary of Key Findings

- Program design broadly meets Australian Government's strategic interests to grow the cyber security workforce to meet the increased demand through a broad range of approaches, including increasing the participation of underrepresented cohorts.
- There are opportunities to expand program scope to support workforce growth, key areas for expansions include cross-skilling to better meet the needs of the evolving sector (e.g. AI, quantum computing, Blockchain and machine learning).
- Other sought-after skills – which are not technology-specific but are valued by employers in the cyber security industry – could also be fostered through the Program. These include: strong problem solving, strategic thinking and communication skills, and a curiosity and eagerness to learn.

Significance

Alignment of the Program with the Government's evolving interest to grow a robust and secure digital economy, and how that can be best achieved being informed by industry, ensures the Commonwealth funds it disburses are optimally allocated to grow the cyber and digital talent pipeline and address the shortage of available workers.

5.1.1.1 On the government's strategic interest in growing a robust and secure digital economy

Growing a robust and secure digital economy is a strategic imperative for the Australian Government. The increasing digitisation of commercial, social and enterprise activities is evolving the threat landscape and diversifying cyber security attack surfaces (10.1.1 refers). The increasing incidence and severity of cyber-crime and state-sponsored cyber-attacks pose threats to Australia's economic and national security (10.1.2 refers). However, there is also economic opportunity in the growing market demand for services that support cyber security risk management (10.1.3 refers).

The government and industry have common interests in addressing barriers and hurdles to the management of national cyber security risks which in turn pose economic security risks to Australia. A central barrier being limits to the capacity of the sector to meet the demand for cyber security services (10.1.4 refers). Another shared challenge lies in addressing social fairness and equity of the industry's growth (10.2 and 10.3 refer). Government has a key role in supporting the training and employment pathways of the cyber security industry (10.3.1 refers); and is seen to be a key partner to the industry in regulating the quality of the cyber security education and training system (10.3.3 refers). Close government-industry collaboration is key to designing policy and programs that resolve barriers to growing the cyber industry underpinning Australia's cyber security posture (10.2 and 10.3 refer).

5.1.1.2 On the Program's design

This evaluation found that the Program's design broadly meets the Australian Government's strategic interests in the cyber security sector (described in the previous section). It does so by supporting the growth of the cyber security workforce through a wide range of approaches (11.1.1 and 11.1.2 refers).

The CSSPIF Guidelines Round 1 and 2, both aimed to improve the future cyber security workforce pipeline by supporting partnerships between industry and education providers, increasing diversity in the cyber security workforce, improving the quality and quantity of cyber security professionals in Australia and funding innovative approaches (Table 7 refers). Between Rounds 1 and 2, the Department altered the Guidelines to expand the focus of the CSSPIF to other underrepresented groups (namely, Indigenous Australia, regional and remote based workers, and neuro diverse individuals), and to limit the eligibility of lead applicants to non-government organisations. The evaluation found that the CSSPIF Grant Guidelines' eligibility requirements align with the Commonwealth Grant Rules and Guidelines.

5.1.1.3 On future focus areas for CSSPIF

There was limited evidence available to suggest that a gap analysis was undertaken to inform program design that otherwise could have identified key areas of need (11.1.2 refers). Stakeholders expressed that a gap analysis would be beneficial and would support the Department to tailor the grant guidelines to the needs of industry and under-represented cohorts. Most stakeholders consulted (n=21, 80.8 per cent) agreed or strongly agreed with the sentiment the CSSPIF should be targeted to specific areas of need in the workforce; and most stakeholders (n=21, 66.6 per cent) also agreed or strongly agreed that changes are required to increase uptake of the Program across the sector (11.1.2 refers). The evaluation found that future focus areas of CSSPIF for the Department to consider include, but are not limited to:

- Thorough industry and marginalised cohort co-design of program guidelines, and participation in assessment committees to evaluate applicant claims (11.1.2 refers).
- Targeting cyber security skill gaps and role profiles identified by the industry as priorities for now and the future (10.1.5 refers to examples highlighted by industry stakeholders).
- Targeting lateral skills of value to the sector, including development of advanced problem solving, communication, strategic thinking and basic cyber security knowledge and skills of the workforce (10.1.5 and 10.2 refer).
- Exploring program design adjustments that could better support the participation of smaller and medium-sized enterprises from the cyber security industry as program applicants and partners (11.1.3 and 11.1.4.2 refer).
- Exploring how the Program can encourage future projects that address workforce retention, and skills for managers in the cyber security industry to operate psychologically secure, diverse and equitable workplaces for all employees (10.1.5-10.1.7 refer).

5.1.1.4 On workforce growth of other digital technology industries

There are opportunities for the Program's scope to support cross-skilling in related fields. Industry stakeholders identified the following skills and occupations that are in demand:

- Secure application developers with skills in Net, Cloud, and Cloud Access and Identity Management;
- Cyber Security Testing, Continuous Monitoring, Management or Governance Systems;
- Cyber security industry and workforce development policy and programs;
- Data Science, AI and the application of machine learning to prevent and identify threats - data science and quantum computing; and
- Blockchain and distributed ledger technologies (10.1.3 and 10.1.5 refer).

Industry representatives reported that they are particularly interested in greater collaboration on initiatives that support cross-skilling that deliver critical skills in emerging technologies, such as AI, blockchain, quantum computing and machine learning (10.2.2 refers).

5.1.2 Key Evaluation Question 2 – Guidelines and Eligibility

How well do the CSSPIF grant opportunity guidelines match the industry's interest in, and capability to, meet the requirements?

- What elements of the program guidelines could be altered to improve its outcomes? (e.g. financial co-contribution, project or eligibility) (guideline impact).
- To what extent did the nature and magnitude of the problem or opportunity that CSSPIF is designed to address change? (guideline effectiveness).
- What opportunities exist for the Program to adapt to the shifting market demand for cyber security professionals? (guideline appropriateness).

Summary of Key Findings

- Current program guidelines attract established industry partners and could better support emerging organisations and novel partnerships.
- Progress on partnerships, funding and projects is evident – even at this relatively early point in time for the Program.
- A risk-based approach to co-contributions and established partnerships with open grant rounds may increase application uptake and support innovation.
- Leveraging industry's goodwill to participate in program co-design will help ensure the CSSPIF remains current and can adapt to meet market demand.

Significance

Firms in the cyber security sector are mostly 'young' (i.e. founded within the past decade) and small (i.e. with fewer than 100 employees). As these attributes tend to hinder their capacity and capability to meet the guidelines and eligibility requirements of the Program, the Program risks unintentionally deterring the largest and most innovative segment of the cyber security and digital industry from participating.

5.1.2.1 On altering elements of the program guidelines to improve outcomes

The evaluation found that the CSSPIF grant opportunity guidelines match industry interest in, but not all of the industry's capability to, meet the requirements. It was observed that:

- The CSSPIF Guidelines are standard and are comparable to other grants programs, but less experienced applicants needed more supportive information to engage in the process (11.1.1 refers).
- The Program's partnerships requirements incentivise collaboration (11.1.4.1 refers).
- The Program's design is broad and inclusive in scope, but some needs of Industry and disadvantaged groups are not met by projects funded to date.
- The Program's design suits a target audience of bigger, better resourced and more experienced applicants (11.1.3 refers).
- The Program's financial requirements mitigate some risks, but may hinder participation from smaller, innovative potential applicants (11.1.4.2 refers).

Firms in the cyber security sector are mostly 'young' (i.e. founded within the past decade) and small (i.e. fewer than 100 employees) (11.1.3 refers). Program eligibility financial requirements are quite high for a sector mostly made up of SMEs: the requirement of the applicant to have at least $500,000 available as 'eligible project expenditure', is an example (11.1.4.2 refers). As these attributes tend to hinder mall-to-medium enterprise's (SME's) capacity and capability to meet the Program guidelines and eligibility requirements, the Program risks unintentionally deterring the largest and most innovative segment of the cyber security and digital industry from participating. Some interviewees believed program eligibility conditions – particularly the co-contribution amounts and financial liquidity assurances – suit larger, more experienced applicants. Some stakeholders were not convinced that favouring larger, more experienced, 'incumbent' applicants would 'shift the dial' in the cyber skills pipeline (11.1.3 refers). The

evaluation found that a risk-based approach to co-contributions and established partnerships with open grant rounds may increase application uptake and support innovation (11.3.1 refers). Leveraging industry's goodwill to participate in program co-design will help ensure the CSSPIF remains current and can adapt to meet market demand and industry capability to meet the requirements (10.2.2 and 10.3.2 refer).

5.1.2.2 On the problem or opportunity that CSSPIF is designed to address

A primary issue challenging Australia's management of national cyber security risks is the capacity of the sector to meet the demand for cyber security services. Current demand for cyber security-skilled labour is greater than the supply of suitably skilled people (10.1.4 refers). Stakeholders expressed the view that, in terms of the nature and magnitude of the problem, the cyber security skills shortage and labour gap is 'not even close' to being addressed, in the words of one interviewee (10.1.4.1 refers). The skills shortage is affecting the cyber security industry's capacity to manage the economic and national security risks from the evolving cyber security threat landscape.

At the same time, the skills shortage impacting the industry at large is affecting the sector's capacity to deliver training that would grow the talent pipeline (10.1.4.2 refers). The pressure to rapidly grow the workforce carries the risk of compromising workforce quality (10.1.4.2 refers). Both are issues that the industry has sought to address on an ad hoc basis (10.2 refers), but which the industry welcomes collaboration with government to coordinate and resolve nationally (10.3.2 refers).

Another imperative for the Program is ensuring the cyber industry grows with social fairness, diversity and equity in mind (10.1.1 refers). Segments of Australian society remain untapped and are underrepresented in the cyber security workforce – and this is an issue the industry has also acknowledged (10.1.6 refers). Overseas research indicates that sustained growth of the cyber security skills pipeline is dependent on making the industry's workplaces psychologically secure, diverse and equitable environments for all employees (10.1.7 refers). Australian data on the nature and magnitude of these demographic diversity and equity issues, and whether they are changing over time, is not widely available. Collection of such data should be addressed by the broader cyber policy community together with industry and civil society.

5.1.2.3 On shifting market demand for cyber security professionals

The high market demand for cyber security professionals and the shortage of available people (10.1.4 refers) has prompted industry to develop their own workforce pipeline initiatives (10.2.1 refers). However, such independent initiatives are not yet fully meeting the need, and could benefit from greater coordination and collaboration as many of these initiatives tend to be ad hoc, or focused on a particular organisation's workforce pipeline rather than the broader sector pipeline (10.2.1 and 10.2.2 refer). While CSSPIF projects have grown and diversified project partnerships over time (11.3.3.2 and 11.4.4 refer), this evaluation found there is still scope for greater collaboration and cooperation in addressing cyber security workforce issues.

Industry stakeholders indicated that their recruitment priorities are for people to fill the following roles:

- 'Oversee and govern' – roles that 'Provide leadership, management, direction, or development and advocacy so the organisation may effectively conduct cyber security work'.
- 'Securely provision' – roles that 'Conceptualise, design, procure, and/or build secure information technology (IT) systems, with responsibility for aspects of system and/or network development'.
- 'Protect and defend' – roles that 'Identify, analyse, and mitigate threats to internal IT systems and/or networks' (10.1.5 refers).

The only expected changes in this prioritisation in the next 3-5 years is the increased importance of 'investigative' roles. Some stakeholders indicated that roles aligned to the 'Operate and Maintain', 'Analyse', 'Collect and Operate', and 'Investigate' National Initiative for Cybersecurity Education (NICE) categories are more likely to need fewer (but highly skilled) human operators in the future. This is because tasks associated with these roles are more amenable to partial or full process automation or assistance from artificial intelligence and machine learning (AI/ML) enabled technology solutions (10.1.5 refers). As noted in section 5.1.1.4, industry stakeholders highlighted secure application development, workforce development, data science, AI, machine learning, quantum computing and encryption and

distributed ledger technologies (e.g. blockchain) are other skills and occupations in demand today or in the future (10.1.3, 10.1.5 and 10.2.2 refer).

5.2 Implementation

5.2.1 Key Evaluation Question 3 – Program Engagement

How well did the Program reach and engage with the intended stakeholders for CSSPIF Rounds One and Two?

- What are some opportunities for future rounds that could enhance program reach, uptake and more quality applications?
- How could a Round Three be better targeted to meet industry needs?

Summary of Key Findings

- Implementation of the Program resulted in engagement with many relevant stakeholders.
- Program reach, uptake and applications quality can be improved.
- CSSPIF could be targeted towards specific areas of industry need. There was limited evidence to suggest that a gap analysis was undertaken to inform program design. There are several implementation considerations to ensure any future grant funding rounds are targeted to the needs of industry.
- Beyond the needs of industry, future rounds need to consider the needs of the disadvantaged cohorts the Program is seeking to support.

Significance

Where an intended audience is not well understood, it is harder to effectively reach, or be sought after by, a large portion of the intended audience. This in turn misses the opportunity to foster greater competition, innovation, and diversity of partnerships that could address the cyber and digital skills pipeline shortages.

5.2.1.1 On enhancing program reach, uptake and more quality applications

This evaluation found that the Program engaged with many relevant stakeholders (11.3.3.2 and 11.4.4 refer). Despite this, there are lessons that could be learned to increase engagement and broaden the reach of the Program in future. This is discussed further in section 5.2.2.2 on program promotion and communications. As mentioned in section 5.1.2.1, there are elements of the Program's eligibility requirements which may have affected the program reach, uptake and applications from SMEs (11.1.4.2 refers), and oriented program communications to target larger, better resourced and more experienced potential applicants (11.1.3 refers). As noted previously, stakeholders consulted for this evaluation mostly agreed that changes to the program are required for the Program to increase uptake across the sector (11.1.2 refers). Greater engagement between the government through co-design processes with industry and civil society could enhance the understanding of the target audience, and to best reach, engage and encourage them to submit quality applications in future rounds.

5.2.1.2 On targeting industry needs in future rounds

As noted previously, stakeholders consulted for this evaluation mostly agreed that the CSSPIF should be targeted to specific areas of need in the workforce (11.1.2 refers).

The needs of industry in terms of sought-after roles and skill types have been discussed already in section 5.1.1.3 regarding future focus areas for CSSPIF, section 5.1.1.4 regarding workforce growth of other digital technology industries, and section 5.1.2.3 regarding the shifting market demand for cyber security professionals.

Beyond skill and role profiles, the industry has other needs that could be addressed in future rounds. It was observed that the CSSPIF application process is standard but poses time and financial barriers that may have deterred participation for SME applicants, or applicants with complicated partnerships and internal governance structures (11.3.1 refers). Stakeholders suggested that the Department hold open grant rounds, referring to the Department of Foreign Affairs and Trade's Australia's Cyber and Critical Tech Cooperation Program as an example. Thous would allow time for potential applicants to raise the significant funds required, establish formal partnerships, and be flexible to support innovation (11.1.4.2 refers).

It is noteworthy that the funds remaining for CSSPIF are significant: to use-up these funds, the Program is dependent on industry capacity to co-invest at least another $34.7M in future funding rounds (11.4.5 refers). It is unknown if the market has this capacity – particularly the sections of the cyber and education sectors the Program has targeted to date. While it is possible that introducing a helpful measure – such as lower minimum co-contribution amounts – could increase SME applications and potentially use up more of the available funds in future rounds; on the other hand, it is also possible that disbursing a greater number of grants with smaller grant amounts would take longer to fully expend program funds.

Beyond the needs of industry, future rounds need to consider the needs of the disadvantaged cohorts the Program is seeking to support. Stakeholders queried as to whether peak bodies and representatives of underrepresented cohorts were consulted on the revised Round 2 Guidelines, considering the revised Guidelines' objective to increase diversity in the cyber security workforce (11.1.2 refers). It was not clear if the Department understood how these cohorts interacted with the cyber security sector and the best ways to involve and engage the cohorts in a meaningful way. Future program grant guidelines should be co-designed with civil society groups representing target groups such as women in Science, technology, engineering and mathematics (STEM), Aboriginal and Torres Strait Islander peoples, neuro-diverse people, and people located in regional and remote areas. Future program funding round assessment committees should also include representatives from such bodies to evaluate applications and verify their methods on how to reach, engage and support disadvantaged groups.

5.2.2 Key Evaluation Question 4 – Program Delivery

How effectively was the Program delivered?

- Was the Program promotion and communication effective?
- How well were risks anticipated, mitigated and managed?

Summary of Key Findings

- Overall, the Program has been effectively delivered in the context of being a new program established during COVID-19 lockdowns.
- Program promotion and communication was adequate but can be improved to increase awareness and visibility of grant recipient partnerships and projects across government and industry.
- Risks for assessments, funding activities and COVID-19 project impacts were managed effectively; risks related to the shortage of suitably qualified trainers needs to be more closely managed in future.

Significance

Well-delivered programs provide assurance that Commonwealth funds are fairly and appropriately disbursed in the Public Interest.

5.2.2.1 On Program delivery

This evaluation found that the Program has been effectively delivered in the context of being a new program established during COVID-19 lockdowns. It was observed that:

- Applicants have responded well to the Program's emphasis on sector diversity in Round 2 (11.3.3.1 refers).

- Applicants have grown and diversified project partnerships (11.3.3.2 refers).
- Over time, a greater number of projects have benefited from larger financial co-contributions from industry (11.3.3.4 refers).

While the quantity of applications reduced between Rounds 1 and 2 (from 55 to 40 applications – 11.3.2 refers), the quantity of applications deemed suitable for funding increased between Rounds 1 and 2 (from 8 to 18 applications – 11.3.3 refers). Most applications between Rounds 1 and 2 were deemed to be suitable (whether funded or not). However, it was also observed that the total number of applications deemed suitable or higher decreased between Rounds 1 and 2 (from 31 to 24) (11.3.3. refers). It was also observed that the CSSPIF application process poses time and financial barriers that may have deterred participation for SME applicants, or applicants with complicated partnerships and internal governance structures (11.3.1 refers). It is possible that these barriers may have influenced the quantity and quality of applications submitted to Round 2.

5.2.2.2 On promotion and communications

Program promotion and communication was adequate but can be improved to increase awareness and visibility of grant recipient projects. It was observed that:

- Additional communications planning resulted in improved coordination, but more can be done to articulate internal roles and responsibilities and set clear expectations for sector engagement (11.2.1 refers).
- Funding round promotion needed planning and input from target audiences to be more effective (11.2.2 refers).
- Stakeholders indicated that it may be beneficial host webinars when funding rounds open, to allow for the intended audience to engage with the Department directly. Stakeholders referred to the Boosting Female Founders Round 2 Webinar as a ‘best practice’ example (11.1.1 refers).

Program communication activities post-funding rounds have been limited, to date. Such activities are an opportunity to nurture knowledge sharing between funded projects and to potentially support the promotion of funded projects and grant funding future rounds among peers (11.2.3 refers).

5.2.2.3 On risk anticipation, mitigation, and management

Financial and COVID-19 pandemic-related risks for assessment and funding activities were managed effectively by the Department (11.1.1, 11.1.4, and 11.3.1 refer). The COVID-19 pandemic has likely affected some potential applicants but has not materially deterred growth in industry co-investment (11.4.6.1 refers).

The Committee’s risk appetite appeared to be influenced by the availability of funds (11.3.3.3 refers). In Round 1, the Department tried to mitigate the risk of over-allocating funds by having stricter criteria thresholds. The Round 1 Assessment Committee’s approach to avoid over-allocation of funds in Round 1 meant that a significant proportion (n=23, 40 per cent) of all Round 1 applications were deemed suitable but were not recommended for funding (11.3.3 refers). While the total number of applications deemed suitable or higher decreased between Rounds 1 and 2 (from 31 to 24) (11.3.3 refers), the average assessment rating value of ‘suitable and recommended for funding’ applications was higher in Round 1 than in Round 2. This may have been influenced by the greater availability of program funding in Round 2.

Although the Department did provide Round 1 applicants feedback on their applications and encouraged applicants to apply for future rounds of funding, it is possible these efforts were insufficient. Round 2 saw five ‘suitable but not funded’ Round 1 applicants re-apply and receive ‘suitable and recommended for funding’ Committee results. However, 18 such applicants from Round 1 did not re-apply (11.3.2 refers). More targeted, early communication with unsuccessful but ‘suitable’ Round 1 applicants after the increased program funding was announced, or even a reconsideration of those ‘suitable but not funded’ Round 1 projects, could have been explored further.

Stakeholders raised the skills shortage for the industry at large as a key risk to CSSPIF Project schedule milestones and outcomes (11.4.6.2 refers). This is discussed further in the next section.

5.2.3 Key Evaluation Question 5 – Environmental Factors

To what extent did the market, policy, economic environment and timing affect performance or quantity and quality of the Program's subscription?

Summary of Key Findings

- Environmental factors appear to have had minimal short-term impact in disrupting program implementation and take up, but project roll-out has been delayed.
- It is unknown how many potential applicants chose not to apply for grants through this Program due to the economic impact of environment factors – including the 2020-21 COVID-19 pandemic public health regulations – which may have reduced their capacity to participate in the Program.
- The skills shortage for the industry at large is a key risk to CSSPIF Project schedule milestones and outcomes.
- The Program is situated in a busy, complicated digital and cyber policy space vying for engagement from industry and key stakeholders

Significance

Small firms (i.e. under 100 employees) – which make up most firms in the cyber industry – have been the hardest hit by the 2020-21 COVID-19 pandemic public health regulations in terms of impact on revenue and business operations, and may have had the least capacity to prepare partnerships and paperwork to apply for the Program.

This evaluation found that the environmental factors appear to have had minimal short-term impact in disrupting program implementation, but project roll-out has been delayed (11.4.6 refers).

The COVID-19 pandemic has likely affected some potential applicants but has not materially deterred growth in industry co-investment (11.4.6.1 refers). It is unknown how many potential applicants chose not to apply for grants through this Program due to the economic impact of environment factors – including the 2020-21 COVID-19 pandemic public health regulations – which may have reduced their capacity to prepare an application to participate in the Program.

The skills shortage affecting the industry at large is a key risk to CSSPIF Project schedule milestones and outcomes (11.4.6.2 refers). The project delays due to role vacancies for cyber security trainers seemed to be unexpected by some projects, or were underestimated in terms of the time it would take to fill the role. Projects based in non-metropolitan areas were most affected by this issue. This is a risk that the assessment committees for future rounds should consider in terms of the feasibility of an application to deliver the project if highly dependent on recruiting cyber security professionals to deliver training.

The Program is situated in a busy, complicated digital and cyber policy space vying for engagement from industry and key stakeholders (10.3.1.1 refers). While many stakeholders noted that there is a lack of clarity on how the programs fit together to address the larger issue (11.4.6.3 refers), it was beyond the scope of this evaluation to explore this issue further.

5.3 Early outcomes of the Program overall

Summary of Key Findings

- Key short-term outputs and outcomes of the CSSPIF Program indicate that the Program is on-track to meet its intended objectives.
- The Program will need to closely monitor whether the funded projects are effectively increasing the participation of key disadvantaged groups.

Significance

The direction of the Program to date being on-track to meet its objectives indicates its propensity to grow the cyber and digital talent pipeline and address the shortage of available workers. This will substantially support the Government's strategic interest in growing a robust and secure digital economy.

Most stakeholders agreed or strongly agreed that the CSSPIF grant program is needed to grow the cyber security workforce and support the sector (11.4.3 refers). Overall, short-term outputs and outcomes of the CSSPIF Program have been largely positive. It was observed that:

- CSSPIF projects are encouraging industry co-investment, which has increased between Rounds 1 and 2 (11.3.3.4 and 11.4.1 refer).
- CSSPIF projects are supporting industry efforts to increase the quality and quantity of cyber security professionals in Australia (11.4.3 refers).
- CSSPIF projects are improving collaboration between industry and the education, training and skills sectors (11.3.3.2 and 11.4.4 refer).

It is encouraging that CSSPIF projects are increasingly responsive to diversity issues in the cyber security workforce (11.3.3.1 and 11.4.2. refer). However, stakeholder opinion is mixed as to whether the CSSPIF's design is conducive to increasing the participation of neuro-diverse people, Aboriginal and Torres Strait Islander people, and women in the cyber security (11.1.2 refers).

At this interim stage, it was beyond the scope of this evaluation to measure and explore medium- and long-term outputs and outcomes of the Program, and outcomes of specific projects.

5.4 Lessons learned from the Program to date and potential for improvement.

Summary of Key Findings

- There continues to be a role for Government in addressing the cyber security skills gap, but this must be done together with industry.
- Future programs addressing the cyber security skills shortage and talent pipeline need to be designed to address the issue of qualified teacher and trainer availability.
- Sustained growth of the cyber security skills pipeline involves encouraging people to stay in that sector, not just training more people to be cyber security professionals.

Significance

The impact of CSSPIF projects in growing a robust and secure digital economy will be partly dependent on greater alignment of coordination of whole-of-economy, State, Territory and industry activities that grow the cyber security and digital talent pipeline in Australia. This strategic alignment and coordination is beyond the scope of the Program and will need to be addressed separately by the policy community and industry at large.

The skills shortage for the industry at large is a key risk to CSSPIF Project schedule milestones and outcomes (10.1.4 refers). The evaluation found that the cyber security skills shortage poses a challenging "catch-22" – where the solution is constrained by the nature of the problem itself:

- On the one hand, the skills shortage is constraining the cyber security industry's capacity to deliver services that manage the economic and national security risks from the evolving cyber security threat landscape (10.1.4.1 refers).
- On the other hand, the skills shortage for the industry at large is constraining the sector's capacity to recruit experienced professionals who can deliver training to the current and future cyber security workforce and grow the talent pipeline needed to manage cyber security risks to our economic and national security (10.1.4.2 refers).

Future programs addressing the cyber security skills shortage and talent pipeline need to be designed to address this latter issue of qualified teacher and trainer availability.

Sustained growth of the cyber security skills pipeline involves encouraging people to stay in that sector, not just training more people to be cyber security professionals. Beyond competitive salaries (10.1.4.2 refers), workforce retention is also dependent on making the industry's workplaces psychologically secure, diverse and equitable environments for all employees (10.1.7 refers). Initial research indicates that large segments of Australian society (e.g. women and people of different ethnic backgrounds) remain underrepresented in the cyber security workforce (10.1.6 refers), in part due to misconceptions, workplace biases and disadvantages (e.g. gender role assumptions, digital literacy and access). More research and data collection into the Australian cyber security industry's diversity and workplace environments is needed.

The role of industry in addressing the cyber security skills gap is key to defining which skills are required, investment, and operating diverse, inclusive and equitable workplaces (10.2 refers). As noted earlier, the cyber security industry (the Industry) is funding and developing its own workforce initiatives to address the skills shortage (10.2.1 refers). However, such initiatives are ad hoc and tend to focus on benefiting their own immediate organisational workforce pipelines, not the sector at large (10.2.2 refers). There is the opportunity for the cyber security industry to collaborate more to address shared problems, like the skills shortage (6.2.3 refers).

Government has a key role in supporting the training and employment pathways of the cyber security industry and providing leadership (10.3 refers). Industry representatives see the government's value lies in creating a coordinated policy context and clear signals to the market; co-investment in best practice; and efficient regulation (10.3.1 refers). Industry representatives welcome the support of government collaboration on issues impacting the sector; and see government as a key partner in regulating the quality of the cyber security education and training system (10.3.2 and 10.3.3 refer).

6 Conclusions

6.1 Context of the Program

The cyber security industry is a diverse niche within the broader digital economy. Firms in this sector vary in terms of service categories, size, revenue, resource capacity, customer bases, and maturity. This makes their requirements for a pipeline of skilled workers equally varied in terms of what knowledge, skills, experience, attributes and qualifications are required or desired to perform the work available now and in the future. Government policies and programs that seek to grow the talent pipeline of this industry need to consider the needs of, and closely involve representatives of, the industry and marginalised groups. This will ensure policy and program design and implementation meets their needs and anticipates their constraints, while also supporting competition, innovation, and diversity.

As the evolving threat environment continues to drive ever more demand for cyber security services, there is an important role for government in collaborating with industry to address the persistent skills shortage in this sector. In some areas, industry has taken its own initiative to foster their own talent pipeline without government support. Where government can make a difference is identifying and addressing gaps industry is not yet investing in, developing and coordinating policies and programs that can support and amplify the impact and effectiveness of industry investments in this talent pipeline.

The impact of CSSPIF projects in growing a robust and secure digital economy will be partly dependent on greater alignment of coordination of whole-of-economy, State, Territory and industry activities that grow the cyber security and digital talent pipeline in Australia. This strategic alignment and coordination is beyond the scope of the Program and will need to be addressed separately by the policy community and industry at large.

6.2 Evaluation of the Program

This evaluation has found that – at this stage – the CSSPIF Program's design and implementation has broadly met its stated objectives. Progress on partnerships, funding and projects is evident – even at this relatively early point in time for the Program. The projects that are funded represent a good spread of activations at various points across the cyber security talent pipeline. In addition, the projects funded – particularly in Round 2 – have clearer plans to increase the participation of disadvantaged or marginalised groups in the sector's workforce.

There is, however, room for improvement in the Program's future. Current program guidelines attract established industry partners with greater resource capacity to participate in the Program. Firms in the cyber security sector are mostly 'young' and small, which hinders their capacity and capability to meet the guidelines and eligibility requirements of the Program as-is. Hence, the Program risks unintentionally deterring the largest and most innovative segment of the cyber security and digital industry from participating. Insufficient advance planning of program communication and promotion activities has made it harder for the Department and promotion partners to effectively reach and appeal to the intended audience. Hence the Program has missed earlier opportunity to foster even greater competition, innovation, and diversity of partnerships that could address the cyber and digital skills pipeline shortages.

The program is still active and has funds remaining, so there is the opportunity to optimise its potential outputs and outcomes. These could include but is not limited to: expanding the Program's reach; addressing gaps not targeted by projects funded in earlier rounds; being more inclusive of smaller enterprises; and fostering networks among program participants.

Key stakeholders have emphasised that there remains a need for this program to support a relatively young industry to grow its talent pipeline and partnerships. Working with key stakeholders to design this future for the Program, while clarifying the scope of intended impact of projects funded through future rounds, will play a valuable role in growing a robust and secure digital economy.

7 Recommendations

Industry feedback indicates that there remains a genuine need and interest in the CSSPIF. This report contains 14 key recommendations for the Department's consideration, which identify improvements to:

- Coordination of government initiatives to grow the cyber security talent pipeline overall;
- Design and delivery of the Program;
- Departmental facilitation of application processes and assessment activities; and
- Tracking program outputs and outcomes.

#	Recommendation	Observation reference #
	Program Design	
1	Key program design features should be retained but lessons learned from funding rounds should be incorporated to ensure alignment with shifting government priorities based on industry need. These activities should: a. Map and analyse other programs across the digital economy to understand specific value-add of CSSPIF in this broader market/system. b. Conduct in-depth market research into who the Program is trying to reach, and market capacity to co-contribute funding to match the volume of available Commonwealth funds. c. Clarify which roles/skills gaps (identified by industry) are to be addressed through future funding rounds. For example, this could involve targeting the higher-priority skills types and novel digital skills, or targeting specific regulatory reforms (e.g. Critical Infrastructure) that require cyber industry workforce support to implement.	10.1.5; 10.3.1.1; 11.1.2; 11.1.3; 11.4.6.3;
2	Co-design future rounds with targeted population segments so the Program can be better informed and promoted to reach and benefit the intended audience. These activities should: a. Identify intended stakeholders to ensure that they are appropriately targeted. b. Co-design the Program's future rounds and any guideline updates with key stakeholder groups to better target the needs of industry and disadvantaged stakeholder groups. This should explore government and industry targets (both realistic and aspirational) in relation to key program outcomes. c. During the development of guidelines, consult with peak bodies and representatives of the underrepresented cohorts that the Program intends benefit.	10.1.5; 10.1.6; 10.1.7; 11.1.3; 11.4.2
3	Explore alternative mechanisms to mitigate risk (e.g. partnership arrangements, co-contributions and liquid assets) as a means of supporting participation of start-ups and niche groups who may find it more difficult to access large amounts of capital that would otherwise enable them to meet co-contribution and liquidity requirements. For example, allow for smaller 'quick win' projects that come with smaller co-contributions amounts (i.e. below $50,000).	11.1.3; 11.1.4.2; 11.3.1; 11.4.5; 11.4.6.1
	Program delivery and implementation	

#	Recommendation	Observation reference #
4	Develop a detailed communications plan in consultation with key stakeholders to ensure the intended audience is being reached. This should include: a. Ensuring that timing of when guidelines are released, applications are due, and implementation milestones are due correspond with optimal marketing events (e.g. Cyber Week) and industry needs (e.g. longer timeframes to prepare applications). b. Hosting webinars to promote the CSSPIF and engage stakeholders in the content prior to application close dates. c. Setting clear intentions, instructions and sought-after outcomes when reaching out through departmental networks to promote the CSSPIF.	10.1.5; 10.1.6; 10.1.7; 11.1.1; 11.1.3; 11.2.1; 11.2.2; 11.2.3; 11.4.2; 11.3.2; 11.3.3.3
5	Seek confirmation from Round 2 grant recipients of their projects' ability to meet their obligations if their project delivery is dependent on expert personnel that are in short supply.	10.1.4.2; 11.4.6.2
6	Clarify forms of acceptable in-kind co-contributions and how to estimate their value.	11.1.1; 11.1.4.2
7	Clarify in the guidelines what is required of applicants to demonstrate how the proposed project will best meet the needs of the intended beneficiary groups.	11.2.2
8	Include representatives from minority or disadvantaged groups in assessment committees to ensure applicants' claims about meeting stakeholder needs are verifiable and appropriate.	11.2.2
	Early outcomes of the Program overall	
9	Establish a CSSPIF Program alumni group to support networking, cross-promotion and shared learnings among grant recipient projects.	11.2.2
10	Reporting on the intended program outcomes and setting year-on-year targets to increase diversity, lift the participation of women, Indigenous Australians, remote based worker and neurodiverse individuals to increase accountability and measure program performance.	11.3.3.1; 11.4.2
11	Track and measure the benefits of the numerous partnerships fostered through this Program.	10.2.2; 11.3.3.2; 11.4.1; 11.4.4
	Lessons learned from the Program to date and potential for improvement	
12	Gather more comprehensive data on the needs and diversity of the cyber security skills pipeline and current workforce.	10.1.4; 10.1.5; 10.1.6; 10.1.7; 10.2.1
13	Map and analyse government cyber security workforce initiatives to identify current and emerging priority areas and better coordinate initiatives across government to target gaps and avoid duplication.	10.3.1.1; 10.3.1.2; 11.4.6.3
14	Stand up an interdepartmental reference group / committee (that also links in with relevant officers from State and Territory Governments) which coordinates policy and programs that serve to grow the cyber security and broader digital workforce.	10.3.1.1; 11.4.6.3

8 Appendix A - Evaluation method

This appendix provides a brief description of the method used to conduct evaluation activities.

8.1.1 Program logic model and theory of change

KPMG created an initial program logic for CSSPIF based on open-source information. A program logic model is a graphical representation of the relationship between program resources, the activities delivered, and the outcomes achieved. The theory of change explains how a program's activities lead to results that may support achieving the program's intended short-, medium and long-term outcomes.

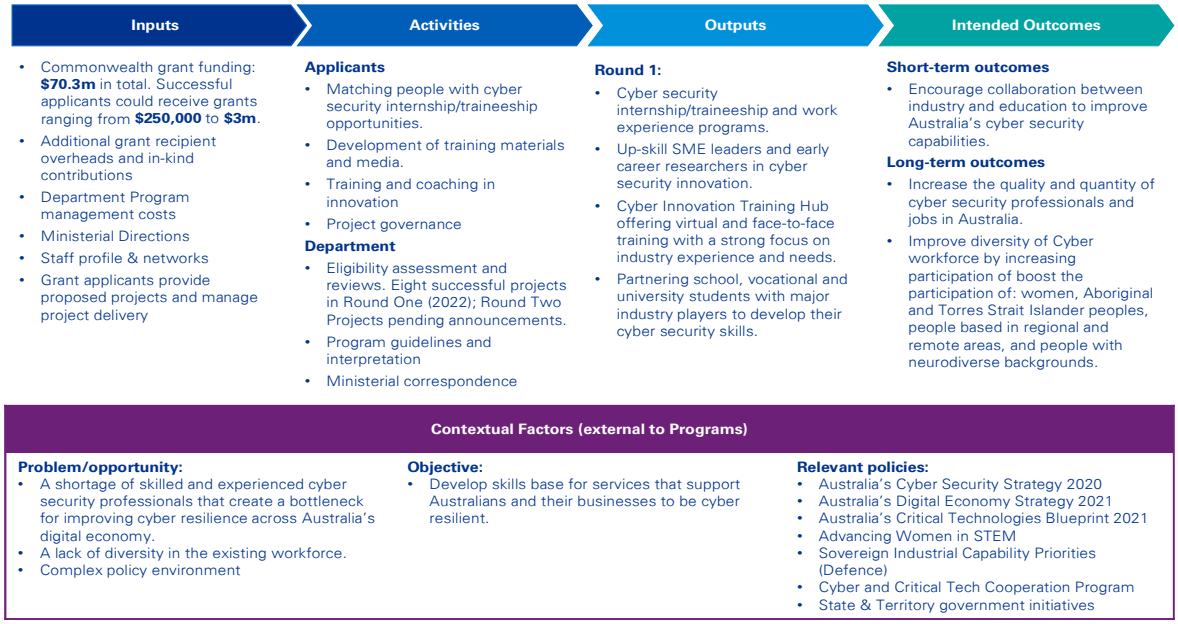


Figure 2: Initial program logic of the CSSPIF.

8.1.2 Stage 1: Evaluation planning and design

This stage included a project initiation meeting and an evaluation design workshop. These meetings aimed to confirm and validate the scope and approach of the evaluation and formed the basis for Stage 2. During this stage, the theory of change, program logic, evaluation questions and data matrix were validated, and the Project Plan, Risk Management Plan and Evaluation Framework were finalised in consultation with the Department.

8.1.3 Stage 2: Conducting the evaluation

This stage included three concurrent streams of work, these were: a desktop scan, stakeholder consultation, and data analysis. The desktop scan involved a review of program documentation and publicly available sources. In addition, a broad range of stakeholders were consulted, including the internal DISR teams, external government departments, grant recipients and relevant industry organisations and representatives. The data collected from these activities, as well as a target survey, informed the data analysis component, leading to the observations detailed in this paper.

8.1.4 Stage 3: Reporting

This stage consolidates the observations and considerations synthesised in Stage 2 into this Report to be presented to the Department. Reporting included:

- Preliminary Findings and Recommendations report, provided to the Department 23 June 2022.
- Draft CSSPIF Evaluation Report, provided to the Department for comment 07 July 2022.
- Final CSSPIF Evaluation Report, provided to the Department 19 July 2022.

8.1.5 Evaluation limitations

Data available to explore potential barriers to submitting grant applications

The information to inform the barriers for potential applicants, was obtained through peak bodies and industry organisations. However, information that would provide further context on these potential barriers, such as consultation with organisations that experienced barriers firsthand, was not obtained as such stakeholders could not be identified and contacted. Instead, the evaluation findings relied on information provided from consultation with CSSPIF grant recipients and industry stakeholders.

Limited access to stakeholders to participate in consultations

- State and territory government representatives were not available to participate in consultations in the time available due to the Federal election and caretaker period coinciding with the consultation period.
- University and vocational institution representatives that were not recipients of grant funding in CSSPIF Round 1 were not available to participate in consultations in the time available due to the Federal election and caretaker period coinciding with the consultation period.
- Round 2 grant recipients were not consulted, as the Government had not yet announced the Round 2 outcomes due to Federal election and caretaker period protocols.

Limited access to program documentation

Documentation provided by the Department was limited in terms of its insight into the program's early design and development processes. Challenges in sourcing such documentation was in part due to staff turn-over in the policy team managing the CSSPIF.

Table 4. CSSPIF Program evaluation questions (per RFQ).

KEQ	Evaluation question*	Considerations	Indicators	Data sources
Design Evaluation				
1	**To what extent does the CSSPIF's design meet the Government's strategic interest in growing a robust and secure digital economy?**	This requires descriptive analysis encompassing: • Documentation of policy and supportive materials. • Analysis of the main activities, including where these were provided and to whom. • Relevant findings from in-flight reviews or similar monitoring and evaluation activity (if undertaken).	• Documentation of the type and availability of all CSSPIF innovative projects awarded and implemented (or in progress of implementation) compared to industry assessment of need. • Criterion based assessment of the extent to which the policy and processes are consistent with Commonwealth Government strategic priorities.	• Grant Opportunity Guidelines; • Project documentation, including project plans, budgets and performance reports; • Stakeholder interviews; and • Market research.
1.1	Are there specific areas of the cyber industry that the CSSPIF could/should be focussed towards?			
1.2	What opportunities exist to expand the scope of the program to support workforce growth of other digital technology industries (e.g. artificial intelligence (AI) and quantum computing)?			
2	**How well do the CSSPIF grant opportunity guidelines match the industry's interest in, and capability to, meet the requirements?**	This will include the following considerations: • Options for future funding allocations. • Opportunities to reduce administration workload for organisations funded in the program and the Department. • Considerations for future program guidelines, including process for conducting future funding rounds. • Areas of higher and lower priority, as identified through stakeholder consultations and desktop review. • Program activities that may not be fully meeting the Program objectives. • Interactions with similar programs (i.e. identifying duplication of activities and/or opportunities to leverage existing funding).	Grantee and Departmental perceptions of the: • Grants process; • Funding allocations; and/or • Administrative requirements for the program.	• Grant Opportunity Guidelines; • Project documentation, including project plans, budgets and performance reports; • Stakeholder interviews; and • Market research.
2.1	What elements (e.g. financial co-contribution, project or eligibility) of the grant opportunity guidelines could be altered to improve its outcomes?			
2.2	To what extent did the nature and magnitude of the problem or opportunity that CSSPIF is designed to address change? What opportunities exist for the program to adapt to the shifting market demand for cyber security professionals?			

KEQ	Evaluation question*	Considerations	Indicators	Data sources
Implementation Evaluation				
3	**How well did the program reach and engage with the intended stakeholders for CSSPIF Rounds One and Two?**	• Areas in which future projects might be funded, where commitments have been made and/or where there are new opportunities for investment.	• Stakeholder perceptions of focus areas for future prioritisation and investment. • Grantee profile and focus areas	• Grant Opportunity Guidelines; • Project documentation, including project plans, budgets, and performance reports; and • Stakeholder interviews.
3.1	What are some opportunities for future rounds that could enhance program reach, uptake and more quality applications?			
3.2	How could a Round Three be better targeted to meet industry needs?			
4	**How effectively was the program delivered and implemented?**	• The extent to which the grantee uses resources available to it to determine and prioritise skills development to increase the pipeline of Australia cyber security professionals, including the type and volume of activity delivered. • Assess grantee delivery of the project in line with documented policies and grant opportunity decision making criteria.	• Extent to which activities have been implemented as planned. • Activities that have been completed. • Stakeholder perceptions on what has impacted achieving the program objectives. • Variation in activities implemented to activities proposed or funded. • Number of grant applications. • Stakeholder perceptions regarding the application process and reasons for applying / not applying. • Whether there is a risk management process in place for the project and criterion-based assessment of its adequacy and whether this is being adhered to.	• Grant Opportunity Guidelines; • Project documentation, including project plans (including any documented risk registers and communication plans), budgets and performance reports; and • Stakeholder interviews.
4.1	Was the program promotion and communication effective?			
4.2	How well were risks anticipated, mitigated and managed?			

KEQ	Evaluation question*	Considerations	Indicators	Data sources
5	**To what extent did the market, policy, economic environment and timing affect performance or quantity and quality of the program's subscription?**	This will encompass: • Alignment of activities implemented with what was identified in project plans/activity work plans, including any changes to activities that were proposed or funded. • External factors that may have impacted, positively or negatively, on achieving the project aims, the delivery of the project and their uptake.	• Stakeholder perceptions on what has impacted achieving the program objectives.	• Grant Opportunity Guidelines; • Project documentation, including project plans, budgets, and performance reports; • Stakeholder interviews; and • Market research.

8.2 Data collection methods

Data collection methods proposed in the table above are described in more detail below.

8.2.1 Desktop review

Program documentation

The Department provided access to available program information on GovTeams to support the evaluation. In total, 70 documents were provided and reviewed to inform the evaluation.

Open-source information

To supplement understanding of the broader strategic context in which the program is operating along with the needs of government and industry, a desktop review of open-sourced information was also undertaken. In total, over 40 open-source references were identified and reviewed to inform the evaluation.

8.2.2 Stakeholder Consultation

Interviews

Throughout the evaluation, 19 interviews were conducted with CSSPIF grant recipients, government officials and industry representatives over a period of 10 weeks from 16 May 2022 to 19 August 2022. Semi-structed interviews were conducted virtually over a one-hour duration with evaluation guidelines and key questions provided to participants in advance.

Industry Workshop

To inform the evaluation, a two-hour workshop with members of the Cyber Security Policy Advisory Network of the Australian Information Industry Association (AIIA) was conducted on 14 June 2022. AIIA is a peak representative body and advocacy group that represents a range of Australia's technology companies and a significant portion of the Australian technology sector workforce. AIIA offered this workshop with their network of members in lieu of an interview with AIIA reps alone, to provide more meaningful insights and contributions to the evaluation. The focus of the workshop was to consider:

- Where in the cyber security industry talent pipeline is industry running its own initiatives to grow the digital/cyber skills pipeline; and
- Identify where the government can best provide support and the external factors impacting industry.

Table 5. Stakeholder map.

Stakeholder Group	Organisation	Individual	Consultation Type
Commonwealth Government	DISR	Representatives from Technology and National Security Division and AusIndustry (3 interviews), including outreach officers	Survey, 3x 1hr interview
	Department of Prime Minister and Cabinet	Representatives	Survey, 1x 1hr interview
	Department of Home Affairs	Representatives and Outreach Officers	Survey, 1x 1hr interview
	Members of the CSSPIF assessment committee(s)	Representatives	Survey, 3x 1hr interview
Grant recipients	LaTrobe University and Wiley	All partners and relevant stakeholders as identified	Survey, 1x 1hr interview
	NSW Treasury	All partners and relevant stakeholders as identified	Survey, 1x 1hr interview

Stakeholder Group	Organisation	Individual	Consultation Type
Relevant peak bodies and other non-Government organisations	CSIRO	All partners and relevant stakeholders as identified	Survey, 1x 1hr interview
	Central Regional TAFE	All partners and relevant stakeholders as identified	Survey, 1x 1hr interview
	TasTAFE	All partners and relevant stakeholders as identified	Survey, 1x 1hr interview
	AustCyber, the Australian Cyber Security Growth Network	All partners and relevant stakeholders as identified	Survey, 1x 1hr interview
	(ISC)2	Representatives	1x 1hr interview
	Council of Small Business Organisations Australia (COSBOA)	Representative	1x 1hr interview
	Trustwave	Representatives	1x 1hr interview
	AIIA	Representatives and facilitators to industry	Survey, 1x 1.5 hr workshop
	Digital Skills Organisation		1x 1hr interview

8.2.3 Surveys

Cyber Security Industry – Workforce Pipeline survey

A survey focused on the activities of industry was sent to all AIIA workshop participants to enable those unable to attend the workshop to provide their input and feedback on industry preferences. A total of 60 surveys were sent out with seven responses received. A copy of the survey is provided at Attachment A.

Cyber Security Skills Partnership Innovation Fund survey

A survey focused on progress towards program outcomes was sent to representatives of the CSSPIF grant recipient organisations and Commonwealth Government agencies to supplement the interview questions. A total of 60 surveys were sent out with 21 responses received. A copy of the survey is provided at Attachment B.

8.3 Analytical Approach

8.3.1 Qualitative information and analysis

Our approach to analysis of the qualitative information was twofold: case studies and thematic analysis.

8.3.1.1 Case studies

Case studies are a powerful mechanism to provide a qualitative illustrative example of the context in which grant funded projects have been delivered and the resulting outcomes that the programs have achieved in aggregate. Case studies were used in the final Evaluation Reports to anchor our recommendations and findings to real people and communities. Primarily, they were prepared using a mixed methods approach including a synthesis of information gathered during our desktop review, stakeholder consultation and quantitative data.

8.3.1.2 Thematic analysis

Thematic analysis of the evidence gathered as it pertains to all domains of enquiry in relation to the relevant evaluation questions set by the Department. This included descriptive information about the CSSPIF program

and individual initiatives and how they are delivered across jurisdictions, factors influencing the effectiveness and efficiency of the programs to achieve the short-term outcomes and identify opportunities for improvement.

8.3.2 Quantitative information and analysis

The Program's and financial data analysis was driven by the four domains of enquiry to understand how the program has been working and identify any improvement opportunities. The program and individual initiative data was analysed using four types of analysis:

- Descriptive analysis, which was used to generate an understanding of the programs, and individual initiatives;
- Process analysis, which was used to generate an understanding of what the program is doing (i.e. Turning inputs into outputs);
- Outcomes analysis, which was used to explore the outcomes being achieved for the Australian community through addressing SME security practices and cyber workforce quality and diversity; and
- Incorporate longitudinal analyses to assess change against the short-term outcomes. This is specifically to determine the change in supply and distribution of supports from grant recipients to the target beneficiaries and identify the impact of grant recipients' funded activities within each program.

The baseline dataset, outcomes reported against existing Key Performance Indicators and the range of program and individual activity guidelines and reporting documentation will form a critical component of this analysis.

8.4 Financial data analysis

The analysis of financial data explores the extent to which the budgeted funding was spent and on the intended activities. At this interim stage it is too early in the Program to build a profile of how and where funding is used against the program's objectives.

9 Appendix B - Index of CSSPIF interviews and workshops

This appendix provides a list of all interviews and workshops conducted with stakeholders consulted to inform this evaluation.

Table 6. Index of CSSPIF interviews and workshops

Label #	Consultation type	Consultation subjects
Consultation A.	Interview	CSSPIF grant recipient
Consultation B.	Workshop	Industry/Sector representative(s)
Consultation C.	Interview	CSSPIF assessment committee representative(s)
Consultation D.	Interview	CSSPIF grant recipient
Consultation E.	Interview	Government representative(s)
Consultation F.	Interview	Industry/Sector representative(s)
Consultation G.	Interview	CSSPIF grant recipient
Consultation H.	Interview	DISR representative(s)
Consultation I.	Interview	CSSPIF assessment committee representative(s)
Consultation J.	Interview	CSSPIF grant recipient
Consultation K.	Interview	DISR representative(s)
Consultation L.	Interview	Industry/Sector representative(s)
Consultation M.	Interview	CSSPIF grant recipient
Consultation N.	Interview	Industry/Sector representative(s)
Consultation O.	Interview	CSSPIF grant recipient
Consultation P.	Interview	CSSPIF assessment committee representative(s)
Consultation Q.	Interview	CSSPIF grant recipient
Consultation R.	Interview	Government representative(s)
Consultation S.	Interview	Industry/Sector representative(s)

10 Appendix C – Observations of the CSSPIF Program Context

This section describes observations regarding the context of the CSSPIF Program that may externally influence the Program Logic and Theory of Change.

10.1 Context: Australia's strategic interest in growing a robust and secure digital economy

10.1 Key Findings

- The increasing digitisation of commercial, social and enterprise activities is evolving the threat landscape and diversifying cyber security attack surfaces.
- The increasing incidence and severity of cyber-crime and state-sponsored cyber-attacks pose threats to Australia's economic and national security; however, they are also contributing factors to the demand for cyber security-skilled people in the workforce.
- Some interview participants noted that they have experienced challenges attracting and retaining cyber security trainers that are a key dependency to deliver their project activities.
- Not all cyber security trainers have contemporary understanding of industry needs.
- The cyber security workforce is not homogenous – it requires a variety of relevant occupations, skills and perspectives, including those associated with policy, legal, risk or education backgrounds.
- Segments of Australian society remain untapped and are under-represented in the cyber security workforce, including, the neurodiverse, Aboriginal and Torres Strati Islander people and women.
- Sustained growth of the cyber security skills pipeline is dependent on making the industry's workplaces psychologically secure, diverse and equitable environments for all employees.

10.1.1 The increasing digitisation of commercial, social and enterprise activities is evolving the threat landscape and diversifying cyber security attack surfaces

Desktop research. Growth and investment in the digital economy to support economic productivity is a key driver for commensurate growth in the cyber security workforce. The pandemic has significantly increased Australia's digitisation and dependence on the internet – to work remotely, to access services and information, and to communicate and continue our daily lives.[1] Fortunately, Australia's economy was reasonably well-positioned in terms of digital readiness.[2] This readiness was advantageous when the COVID-19 pandemic lockdowns and social distancing rules of 2020-21 accelerated technology adoption as firms were forced to

[1] ACSC. 2021. *ACSC Annual Cyber Threat Report*. pp 8. 1 July 2020 to 30 June 2021. Retrieved from: https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21
[2] Cisco. 2019. *Digital Readiness Index*. Retrieved from: https://www.cisco.com/c/dam/en_us/about/csr/reports/global-digital-readiness-index.pdf

experiment with remote working – with up to 40 per cent of employed people working from home.[3] As shown in Figure 3, most industries (except for the construction, and transport, postal and warehousing industries) increased their share of remote working capacity by a significant margin (i.e. greater than 10 per cent) in response to the pandemic.

This accelerated digitisation has increased the attack surface and generated more opportunities for malicious cyber actors to exploit vulnerable targets in Australia. The Australian Cyber Security Centre (ACSC) identified the following key cyber security threats and trends in the 2020–21 financial year:

- Exploitation of the pandemic environment;
- Disruption of essential services and critical infrastructure;
- Ransomware – which has grown in profile and impact, and poses one of the most significant threats to Australian organisations;
- Rapid exploitation of security vulnerabilities;
- Supply chains – particularly software and services – continue to be targeted by malicious actors as a means to gain access to a vendor's customers; and
- Business email compromise.[4]

These threats and trends are in part driven by challenges that businesses have faced in keeping remote workplaces secure. These challenges include, but are not limited to:

- Rapid deployment of new collaboration tools, like video conferencing;
- Lack of security awareness among the remote workforce;
- Keeping up with the new threats and tactics;
- Concern over physical security with so many distributed assets; and
- Strain on help desk teams from an influx of remote work complications.[5]

Stakeholder interviews. Industry and government stakeholders consulted for this evaluation have called out these risks and issues as contributing factors to the demand for cyber security-skilled people in the workforce.[6]

[3] Productivity Commission. 2021. *Working from home*. Research paper. pp 2. Retrieved from: https://www.pc.gov.au/research/completed/working-from-home
[4] ACSC. 2021. *ACSC Annual Cyber Threat Report*. 1 July 2020 to 30 June 2021. Retrieved from: https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21
[5] ISC^2. 2021. *ISC^2 Cybersecurity Workforce Study*. pp 0-31. Retrieved from: https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx
[6] Consultation B, Consultation E, Consultation F, Consultation I.

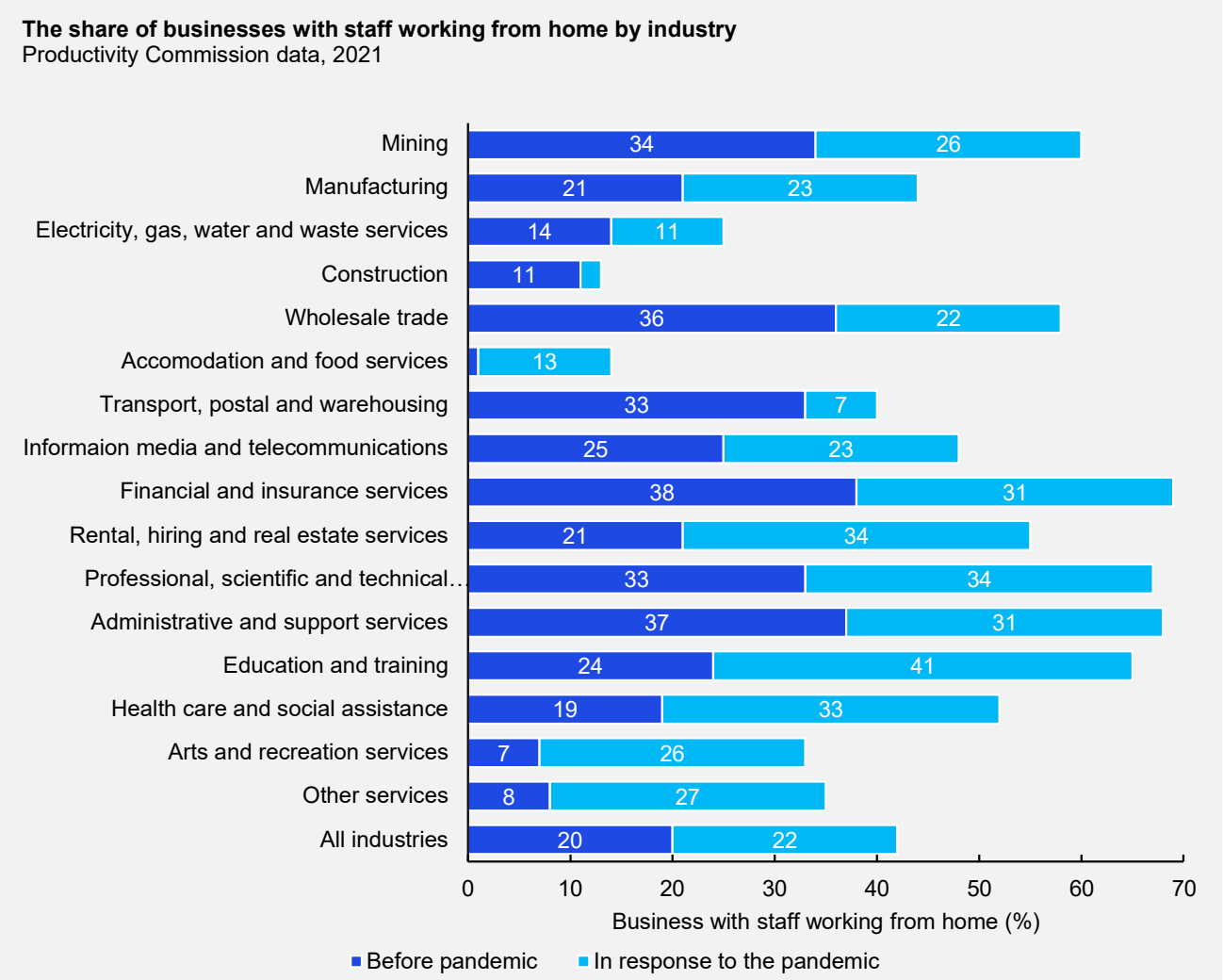


Figure 3. Productivity Commission data reflecting the share of businesses with staff working from home by industry, April 2021. (Source: Figure 1.4 in Productivity Commission (2021) 'Working from home' research paper).

10.1.2 The increasing incidence of cyber-crime and state-sponsored cyber-attacks pose threats to Australia's economic and national security

Desktop research. Increasing incidence of cyber security events are also a key driver for commensurate growth in the cyber security workforce. The ACSC received one cybercrime incident report every eight minutes in 2020-21. This period experienced a near 13 per cent increase in the volume of reports, and a greater proportion of these reports were categorised by the ACSC as 'substantial' in their impact.[7]

> *No sector of the Australian economy was immune from the impacts of cybercrime and other malicious cyber activity. Government agencies at all levels, large organisations, critical infrastructure providers, small to medium enterprises, families and individuals were all targeted over the [… 2020-21] reporting period – predominantly by criminals or state actors.*[8]

Interviews. Industry and government stakeholders consulted for this evaluation have called out these trends as contributing factors to the demand for cyber security-skilled people in the workforce.[9]

[7] ACSC. 2021. *ACSC Annual Cyber Threat Report*. 1 July 2020 to 30 June 2021. pp 8. Retrieved from: https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21
[8] ACSC. 2021. *ACSC Annual Cyber Threat Report*. 1 July 2020 to 30 June 2021. pp 8. Retrieved from: https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21
[9] Consultation B, Consultation E, Consultation F, Consultation I.

[The] Cyber security threat for small businesses is heightened by international issues and increased digitisation. […] Small businesses are vulnerable – they're seen by threats as a 'way in' to the supply chain.[10]

10.1.3 There is economic opportunity in the growing market demand for services that support cyber security risk management

Desktop research. Between 2017 and 2020, global spending on cyber security grew from US$113 billion to US$147 billion.[11] It is expected that global spending on cyber security will reach US$207 billion by 2024.[12] Australian businesses are tapping into the growing need for cyber security products and services. In 2020, Australian cyber security providers generated A$3.6 billion in revenue – A$3 billion from the domestic market and A$600 million from international markets.[13] Australians spent approximately A$5.6 billion on cyber security from local and international providers in 2020.[14] The gross value added of Australia's cyber security sector in 2020 was approximately A$2.3 billion.[15] A greater focus on cyber security by Australian businesses is forcast to see significant benefits to the wider economy, and could lift business investment by 5.5 per cent by 2030, creating 60,000 new jobs.[16]

Interviews. Several stakeholders who were consulted noted the economic opportunity for Australian firms in responding to the demand for services that support cyber security risk management.

There has been massive growth in cyber consulting – in risk consulting, especially.[17]

Start-ups are looking to develop [… novel cyber security] technologies in conjunction with [our organisation].[18]

10.1.4 Current demand for cyber security-skilled labour is greater than the supply of suitably skilled people

10.1.4.1 The skills shortage is affecting the cyber security industry's capacity to manage the economic and national security risks from the evolving cyber security threat landscape

Desktop research. There are approximately 46,946 people employed in the cyber security workforce.[19] Demand is out-stripping the supply of candidates, with cyber security workforce job vacancies (n=6,535) accounting for over a tenth of all cyber security jobs available – that is, 12.2 per cent of all 53,481 jobs (including vacancies).[20] This imbalance is more than four-times higher than vacancy rates for rest of the economy: Labour Account data shows that whole-of-economy job vacancies accounted for 2.7 per cent of all jobs in the December quarter 2021.[21, 22]

[10] Consultation F.
[11] AustCyber. 2020. *Australia's Sector Competitiveness Plan 2020, Executive Summary*. Retrieved from: https://www.austcyber.com/resources/sector-competitiveness-plan/executive-summary
[12] Gartner. 2020. *Forecast: Information Security and Risk Management, Worldwide, 2018-2024, 2Q20 Update*. Retrieved from: https://www.gartner.com/en/documents/3988093
[13] AustCyber. 2020. *Australia's Sector Competitiveness Plan 2020, Plan at a Glance*. Retrieved from: https://www.austcyber.com/resources/sector-competitiveness-plan/plan-at-a-glance
[14] AustCyber. 2020. *Australia's Sector Competitiveness Plan 2020, Plan at a Glance*. Retrieved from: https://www.austcyber.com/resources/sector-competitiveness-plan/plan-at-a-glance
[15] AustCyber. 2022. *Australia's Cyber Security Sector Competitiveness Plan - 2020 Update: Driving growth and global competitiveness*. Retrieved from: https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2020
[16] Deloitte Access Economics, and the Australian Computer Society. 2021. *ACS Australia's Digital Pulse 2021*. Retrieved from: https://www2.deloitte.com/au/en/pages/economics/articles/australias-digital-pulse.html
[17] Consultation D.
[18] Consultation M.
[19] AustCyber. 2022. *AUCyberExplorer Cyber security Supply And Demand Heat Map*. Accessed 22 July 2022. Retrieved from: https://www.aucyberexplorer.com.au/heatmap.html
[20] AustCyber. 2022. *AUCyberExplorer Cyber security Supply And Demand Heat Map*. Accessed 22 July 2022. Retrieved from: https://www.aucyberexplorer.com.au/heatmap.html
[21] Australian Bureau of Statistics. 2022. *Job Vacancies, Australia. February 2022*. Link: https://www.abs.gov.au/statistics/labour/jobs/job-vacancies-australia/latest-release
[22] Australian Bureau of Statistics. 2021. *Labour Account Australia. Reference period: December 2021*. Link: https://www.abs.gov.au/statistics/labour/labour-accounts/labour-account-australia/dec-2021

Survey responses. Most (56.7 per cent, n=21) respondents to the CSSPIF survey disagreed or strongly disagreed with the statement that 'there are sufficient people in the workforce to pursue a cyber security career' (Question 26).[23]

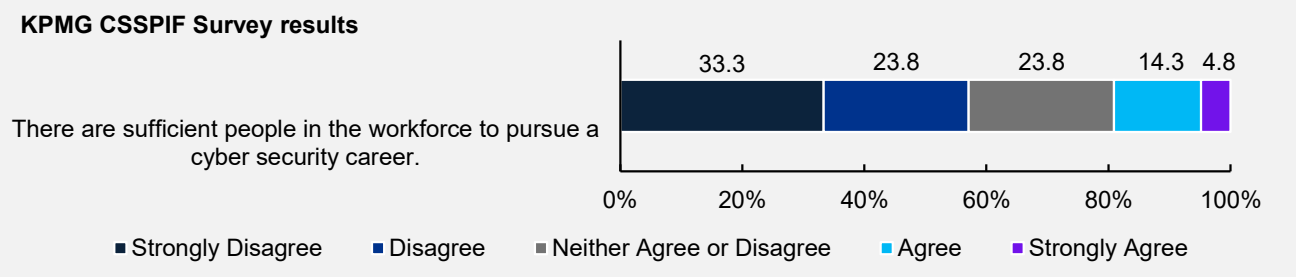


Figure 4: KPMG CSSPIF Survey, question 26: 'There are sufficient people in the workforce to pursue a cyber security career'. (Source: KPMG CSSPIF Survey Question 26, 2022).

Interviews. Numerous government and industry stakeholders interviewed for this evaluation expressed the view that the cyber security skills shortage and labour gap is 'not even close' to being addressed, in the words of one interviewee. Interviewees also expressed the view that demand for the cyber security workforce and reliance on the workforce pipeline is expected to increase. Two Interviewees raised the REDSPICE Budget 2022-23 as a policy and program that will have a significant impact on existing skills shortages in the cyber and broader digital labour market in Australia.[24] It was also noted by interviewees that there is a lot of competition for skilled labour in the digital economy overall, including but not limited to cyber security.[25]

10.1.4.2 The skills shortage for the industry at large is affecting the sector's capacity to deliver training that would grow the talent pipeline

Desktop research. It is difficult to find and recruit qualified cyber security professionals. Globally, 60 per cent of leaders expressed that their organisations struggle with recruitment.[26] In particular, registered training organisations (RTOs) struggle to recruit and retain experienced trainers capable of offering higher-level ICT certificates (and specialisations). DSO's *Towards a New Model for the Development of Digital Skills Discussion Paper* outlines that:

> *… remuneration offered by RTOs for trainers may largely influence retention, for example, a cyber security specialist can earn $180,000 in industry but only $100,000 in an RTO.*[27]

Effective training is dependent on teaching and mentoring interactions with industry professionals who have relevant experience in the subject matter. Students cannot be effectively taught cyber security in a passive classroom setting because the cyber sector evolves too fast. Not only are there not enough appropriately skilled educators to keep up with demand, but new cyber threats emerge every day and educators and curriculums cannot adapt fast enough to keep up.[28]

Interviews. Stakeholders agreed with desktop research findings and noted that there is a significant salary gap between industry and the education sector and reiterated that education providers experience difficulties with the recruitment of appropriately skilled trainers.[29] Stakeholders also expressed the sentiment that trainers do not necessarily have a contemporary understanding of industry needs.

Industry stakeholders expressed particular concern about how difficult it is to find suitably experienced mentors and educators.[30] One stakeholder highlighted additional issues surrounding assurance of those trusted to provide quality training.

[23] KPMG CSSPIF Survey Question 26. See Attachment B.
[24] Consultation E, Consultation R.
[25] Consultation R.
[26] Fortinet. 2022. 2022 *Cybersecurity Skills Gap Global Research Report*. pp 10. Retrieved from: https://mysecuritymarketplace.com/mp-files/2022-cybersecurity-skills-gap.pdf/
[27] Digital Skills Organisation, 2021. Towards a new model for the development of digital skills 2021. pp 17. Retrieved from: https://digitalskillsorg.com.au/assets/pdf/Digital_Skills_Organisation_Discussion_Paper.pdf
[28] Cybint. 2019. Cybersecurity Education: Why Universities are Missing the Mark. Accessed 7 June 2022. Retrieved from: https://www.cybintsolutions.com/cybersecurity-education-why-universities-are-missing-the-mark/
[29] Consultation I, Consultation L, Consultation O.
[30] Consultation C, Consultation G, Consultation S.

[There are] Issues with micro-credentials around who can be trusted to provide quality training. […] Industry is screaming for skilled workers but the focus on quality must remain.[31]

Stakeholders have highlighted that Australia has a good reputation for the quality of its cyber security workforce, and that workforce quality needs to be maintained while also working to grow the talent pipeline of the cyber security industry.[32]

10.1.5 The cyber security workforce is not homogenous – it requires a variety of relevant occupations, skills and perspectives

Desktop research. There are several cyber security skills frameworks which illustrate the diversity of occupations and skills in the sector. Two examples stakeholders often referred to throughout the consultation process were the Australian Signals Directorate (ASD)'s Cyber Skills Framework and the US Government's Workforce Framework for cyber security from the NICE (the "NICE Framework").[33, 34] Globally, most cyber security professionals see themselves fitting within the following top-three NICE Framework categories:

- 'Oversee and govern' (28 per cent) – roles that 'Provide leadership, management, direction, or development and advocacy so the organization may effectively conduct cyber security work'.
- 'Securely provision' (18 per cent) – roles that 'Conceptualise, design, procure, and/or build secure information technology (IT) systems, with responsibility for aspects of system and/or network development'.
- 'Protect and defend' (16 per cent) – roles that 'Identify, analyse, and mitigate threats to internal IT systems and/or networks'.[35, 36]

Other common misconceptions include "cyber security is only a job in an IT team" or "a job in cyber security means you must join the defence force". On the required skills front, it is common to hear "you need to be able to code" or "you have to study at university for a really long time". Busting these and other myths about cyber security careers is crucial for attracting the right talent into the industry. It is important to communicate the plethora of career opportunities in cyber security that don't have a technical focus but rather require people with a policy, legal, risk or education background.[37]

Survey. Industry responses to the Cyber Security Industry Workforce Pipeline Survey indicated that the prioritised future demands for skill categories (per the NICE Framework) bears similarities to current demands for the Australian industry (see Figure 5). A key difference between current and future demand (according to the survey data) is an expected increase in demand for 'oversee and govern' roles and associated leadership, management, direction, or development skills (see Figure 6).

[31] Consultation S.
[32] Consultation I, Consultation S.
[33] ASD. 2020. ASD Cyber Skills Framework. Retrieved from: https://www.cyber.gov.au/acsc/view-all-content/publications/asd-cyber-skills-framework
[34] United States' National Institute of Standards and Technology (NIST). 2020. Workforce Framework for Cybersecurity (NICE Framework). NIST Special Publication 800-181, Revision 1. Retrieved from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf
[35] ISC^2. 2021. *ISC^2 Cybersecurity Workforce Study*. pp. 30-31. Retrieved from: https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx
[36] United States' National Institute of Standards and Technology (NIST). 2020. *Workforce Framework for Cybersecurity (NICE Framework). NIST Special Publication 800-181*, archived. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf
[37] Owen Pierce. (2018). *Building the cyber security workforce Australia needs*. The Good Universities Guide. Retrieved from: https://www.gooduniversitiesguide.com.au/education-blogs/guest/building-the-cyber-security-workforce-australia-needs

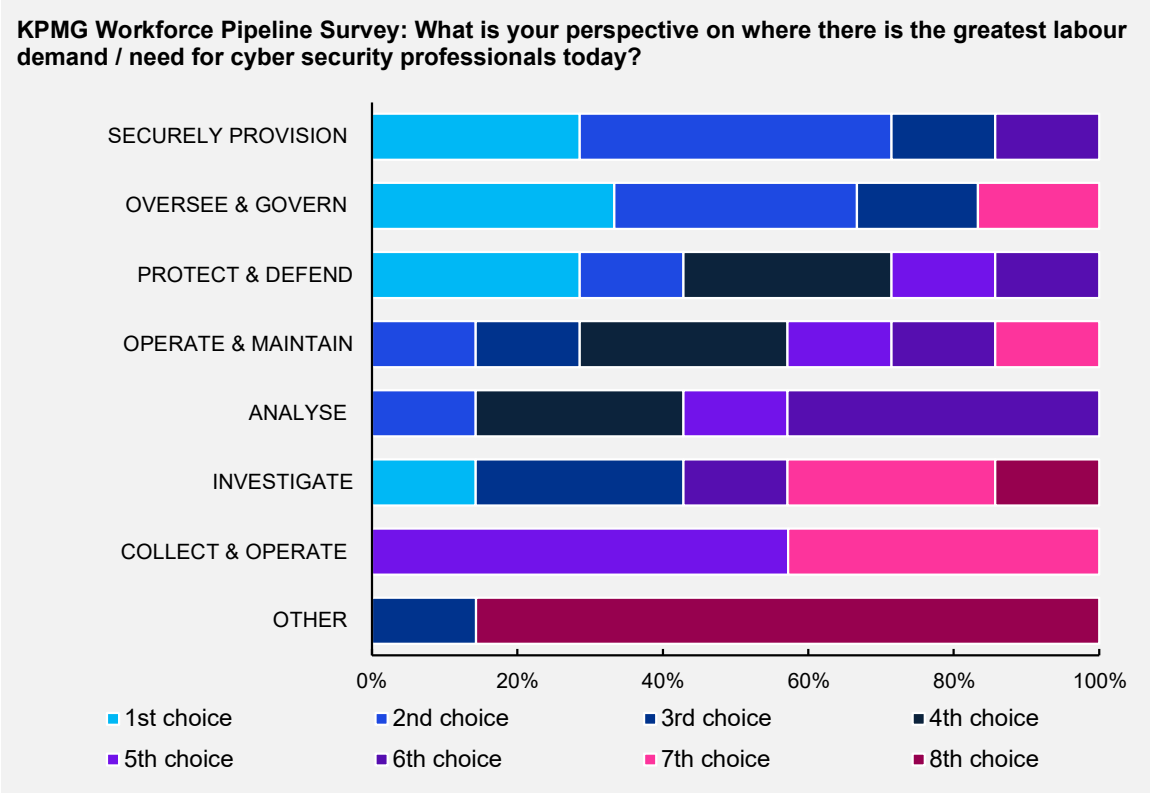


Figure 5. KPMG Cyber Security Industry Workforce Pipeline Survey Question 2: What is your perspective on where there is the greatest labour demand / need for cyber security professionals today? (Source: KPMG Cyber Security Industry Workforce Pipeline Survey Question 2, 2022, n=7).

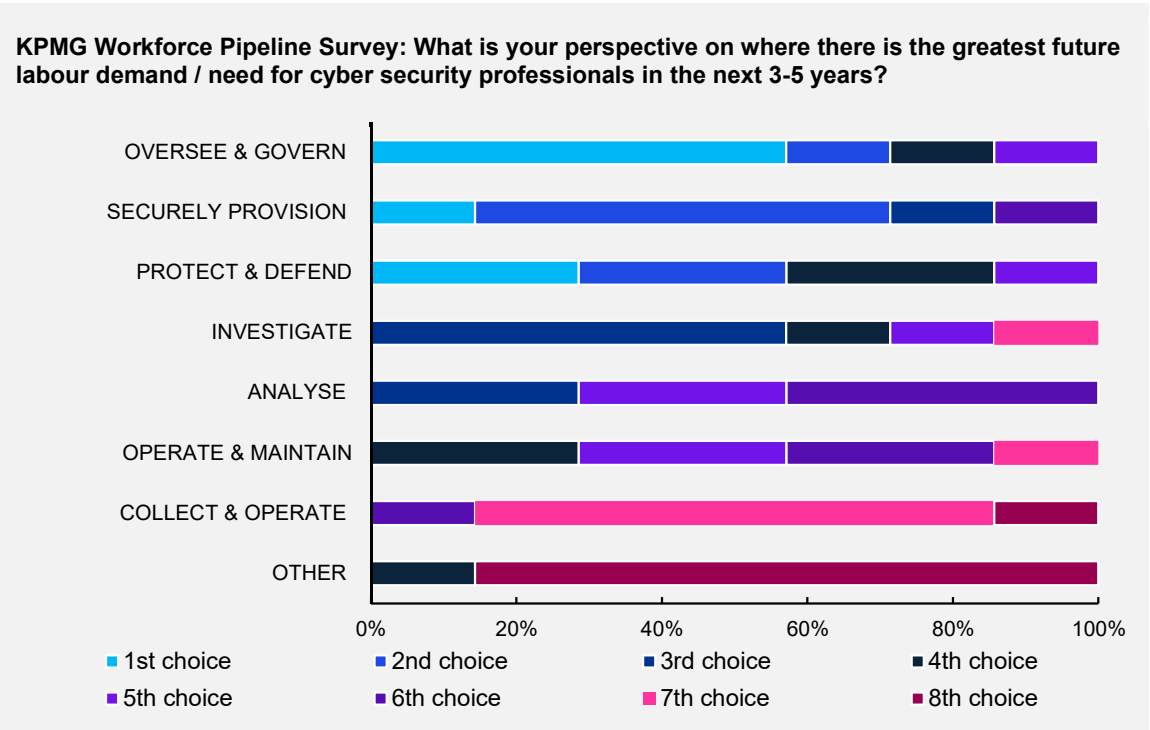


Figure 6. KPMG Cyber Security Industry Workforce Pipeline Survey Question 4: What is your perspective on where there is the greatest future labour demand / need for cyber security professionals in the next 3-5 years? (Source: Cyber Security Industry Workforce Pipeline Survey Question 4, 2022, n=7).

Responses to this latter survey highlighted the following as other skills or occupations in demand today or in future from the cyber security industry:

- Ability to provide advice to governments (in Australia and overseas).
- Secure application developers with skills in Net, Cloud, and Cloud Access and Identity Management.
- Cyber Security Testing, Continuous Monitoring, Management or Governance Systems.
- Cyber security industry and workforce development policy and programs.
- Data Science, AI and the application of machine learning to prevent and identify threats - data science and quantum computing.
- Blockchain and distributed ledger technologies (see Attachment A).

Stakeholder opinion is split on whether government support for growing the cyber security workforce should be broad and inclusive of all roles, occupations and associated skills, or more focused. Slightly more CSSPIF survey respondents (80.9 per cent; n=17) agreed or strongly agreed with the statement 'CSSPIF should be targeted to specific areas of need in the workforce' than those who agreed or strongly agreed (71.4 per cent; n=15) with the statement 'The CSSPIF should be broad to increase participation across the cyber security workforce'.[38]

Interviews. Industry representatives consulted for this evaluation indicated that roles aligned to the 'Operate and Maintain', 'Analyse', 'Collect and Operate', and 'Investigate' NICE categories are more likely to need fewer but highly skilled human operators as tasks associated with these roles are more amenable to partial or full process automation or assistance from AI/ML enabled technology solutions.[39]

10.1.6 Segments of Australian society remain untapped and are under-represented in the cyber security workforce

Desktop research. Australia is a diverse society, and increasingly so.

On gender: Slightly more than half (50.7 per cent) of all Australians are women.[40] Research from 2020 found that women account for a slightly greater share (27.2 per cent) of the Australian cyber security sector workforce than the global average (25 per cent). [41] [42] This is also a greater share than the total Information and Communications Technology (ICT) workforce (21.8 per cent), but women's representation is lower than in the broader information, media and telecommunication sector (39.2 per cent) and significantly lower than the share of women in the population. Data on non-binary sex peoples in Australia and the Australian ICT and cyber security sector are not yet available.[43]

On cultural and linguistically diverse backgrounds: 3.2 per cent of Australians identify as Aboriginal and Torres Strait Islander peoples; and most (51.5 per cent) Australian residents were born overseas or are children of immigrants, with England, India, China and New Zealand representing the most common countries of birth (outside Australia) for Australians.[44] Data on the representation of cultural and linguistically diverse groups – including Aboriginal and Torres Strait Islander peoples – in the ICT and cyber security industry in Australia are not yet available.

On neurodiversity: Estimates on neurodiversity indicate that 1-1.5 per cent of the population are on the Autism Spectrum: around 1 in 42 males and 1 in 189 females.[45] In 2015, there were 164,000 Australians with Autism. Nearly a third (31 per cent) of participants in the Australian National Disability Insurance Scheme (NDIS) are on the Autism Spectrum, and around 1 in 50 Australian school children has a formal autism diagnosis and are registered to receive Carer Allowance.[46] Data on the representation of these groups in the ICT and cyber security industry in Australia are not yet available.

Interviews. Industry confirmed the need to better support disadvantaged groups, notably women and recognise there is untapped segments of society with barriers to workforce entry.[47]

[38] KPMG CSSPIF Survey Questions 4 and 5. See Attachment B.
[39] Consultation B.
[40] Australia Bureau of Statistics. 2021. 2021 Census. Retrieved from: https://www.abs.gov.au/census/find-census-data/search-by-area
[41] AustCyber. 2022. *Australia's Cyber Security Sector Competitiveness Plan - 2020 Update: Driving growth and global competitiveness*. Retrieved from: https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2020
[42] ISC². 2021. ISC² Cybersecurity Workforce Study. pp. 11. Retrieved from: https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx
[43] Australia Bureau of Statistics. 2021. 2021 Census. Retrieved from: https://www.abs.gov.au/census/find-census-data/search-by-area
[44] Australia Bureau of Statistics. 2021. 2021 Census. Retrieved from: https://www.abs.gov.au/census/find-census-data/search-by-area
[45] Australia Bureau of Statistics (2017), NDIS Quarterly Report (June 2015), A4 Autism Aspergers Advocacy Australia (2015).
[46] Australia Bureau of Statistics (2017), NDIS Quarterly Report (June 2015), A4 Autism Aspergers Advocacy Australia (2015).
[47] Consultation D, Consultation N, Consultation R.

10.1.7 Sustained growth of the cyber security skills pipeline is dependent on making the industry's workplaces psychologically secure, diverse and equitable environments for all employees

Desktop research. Discrimination is a potential cause of talent loss for the cyber security sector. Data from the United Kingdom indicated that the groups most likely to experience discrimination in the cyber security workforce were gender diverse people (e.g. non-binary, trans and other genders) and people of colour (notably, people with Black/African/Caribbean and Asian ethnic heritage).[48] This same National Cyber Security Centre (NCSC) survey found that one in ten (9 per cent) cyber industry employees have considered leaving their employer or the industry due to diversity and inclusion issues. A challenge is that some in the industry also perceive organisational efforts to make the workplace more equitable to be a threat to their own career progression and position. Similar data is not yet available for the Australian industry.

International and Australian research has shown that there are intersectional factors that hinder participation of some groups in the cyber security labour force which must be considered to effectively improve their representation. One of the largest of these intersectional factors is the perception of cyber security as a career option for people other than men or existing IT professionals. According to the Director of Cyber Security Advocacy for the Asia-Pacific Region at (ISC)², Tony Vizza:

> *The biggest challenge in terms of diversity is the long standing perception that cyber security is something that boys do; something that men do. [That] It isn't something that girls do.*[49]

Jane Landon, Applied AI Operations at Penten, writes in a 2021 article that bridging the gender gap at senior levels is also a known issue:

> *The appointment of women at the highest levels of Australia's cyber security sector also underscores the value of non-tech skills – including leadership – in cyber security.* [50]

An issue that the sector struggles with is welcoming people with diverse backgrounds into its workforce, putting barriers up before someone even has the opportunity to try their hand at a role in cyber security.[51]

> *Screening people to the degree the sector does, is working against every grain of what diversity really means, by excluding those who cannot afford a high-level tertiary education but might have the skills and attitude to learn the craft on the job.*[52]

For example, statistics from the National Indigenous Australians Agency's Indigenous Digital Inclusion Plan discussion paper[53] indicates that, based on data from the Australian Digital Inclusion Index (ADII), Aboriginal and Torres Strait Islander people are 7.8 points behind the national average (76.3 points) for access to digital devices and services, 6.9 points behind the national average (60.9 points) for affordability of digital devices and access, and 9.2 point behind the national average (52 points) for digital ability. This paper also shows that the ADII access gap between Indigenous Australians and the national average has been widening over time (5.2 points in 2018; 7.3 points in 2019; and 7.8 points in 2020). Such factors reduce the likelihood of and opportunities for people from Indigenous communities to join Australia's cyber security workforce.

Globally, key investments that organisations are making to address the cyber security skills diversity gap include, but are not limited to:

- Invest in training;
- Provide more flexible working conditions;
- Invest in certifications;
- Invest in diversity, equity, and inclusion initiatives;

[48] National Cyber Security Centre UK. 2020. *Decrypting Diversity: Diversity and Inclusion in Cyber Security*. pp. 7. Retrieved from: https://www.ncsc.gov.uk/files/Decrypting-Diversity-v1.pdf
[49] AustCyber. (2021 July 2). *How to improve diversity and workplace culture in the cyber security sector*. Retrieved from: https://www.austcyber.com/news-events/how-improve-diversity-and-workplace-culture-cyber-security-sector
[50] Landon, J. (2021 September 3). *Lifting Diversity Essential to Australia's Cyber Drive*. Cyber Security Connect. Retrieved from: https://www.cybersecurityconnect.com.au/industry/7115-lifting-diversity-essential-to-australia-s-cyber-drive.
[51] AustCyber. (2021 July 2). *How to improve diversity and workplace culture in the cyber security sector*. Retrieved from: https://www.austcyber.com/news-events/how-improve-diversity-and-workplace-culture-cyber-security-sector
[52] AustCyber. (2021 July 2). *How to improve diversity and workplace culture in the cyber security sector*. Retrieved from: https://www.austcyber.com/news-events/how-improve-diversity-and-workplace-culture-cyber-security-sector
[53] National Indigenous Asutralians Agency. 2021. *Indigenous Digital Inclusion Plan – Discussion Paper*. Retrieved From: https://www.niaa.gov.au/sites/default/files/publications/indigenous-digital-inclusion-plan-discussion-paper.pdf

- Hire for attitude and aptitude, and train for technical skills;
- Provide well-defined career paths;
- Encourage women and minorities to pursue STEM degrees in college;
- Establish organisational diversity goals;
- Establish mentorship programs; and
- Address pay and promotion gaps, if they exist.[54]

For example, companies who had tried to build a neurodiverse workforce were required to adjust their processes for managerial support, advocacy and policy, accommodating individual needs, and recruitment.[55] Graduates of Australia's increasingly diverse cyber education pipeline will expect an organisational culture that supports – and even celebrates – this diversity and inclusion.

Interviews. Industry confirmed the need to better support disadvantaged groups, notably women and recognise there is untapped segments of society with barriers to workforce entry.[56]

10.2 Context: The role of industry in addressing the cyber security skills gap

10.2 Key Findings

- The education sector faces challenges in recruiting and retaining trainers with relevant skills in cyber security due to the speed at which the industry moves.
- The cyber industry is funding and developing their own workforce pipeline initiatives to support the cyber security workforce pipeline.
- There is the opportunity for the cyber security industry to collaborate more to address shared problems.

Survey responses. Respondents to the Cyber Security Industry Workforce Pipeline Survey indicated that they see the role of industry to be in developing problem solving, communication, strategic thinking and basic cyber security knowledge and skills of the workforce. This is detailed in Figure 7 below. In addition to this, 26 per cent of participants felt that more should be done to develop workforce skills using both internally delivered (by employers) and informal on-the-job training mechanisms. This is detailed in Figure 8 below.

[54] ISC^2. 2021. ISC^2 Cybersecurity Workforce Study. pp. 22. Retrieved from: https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx
[55] Eleanor T. Loiacono. 2018. *Building a Neurodiverse High-tech Workforce*. Retrieved from: https://www.researchgate.net/profile/Eleanor-Loiacono/publication/329458841_Building_a_Neurodiverse_High-tech_Workforce/links/5c671ab092851c1c9de45108/Building-a-Neurodiverse-High-tech-Workforce.pdf
[56] Consultation B.

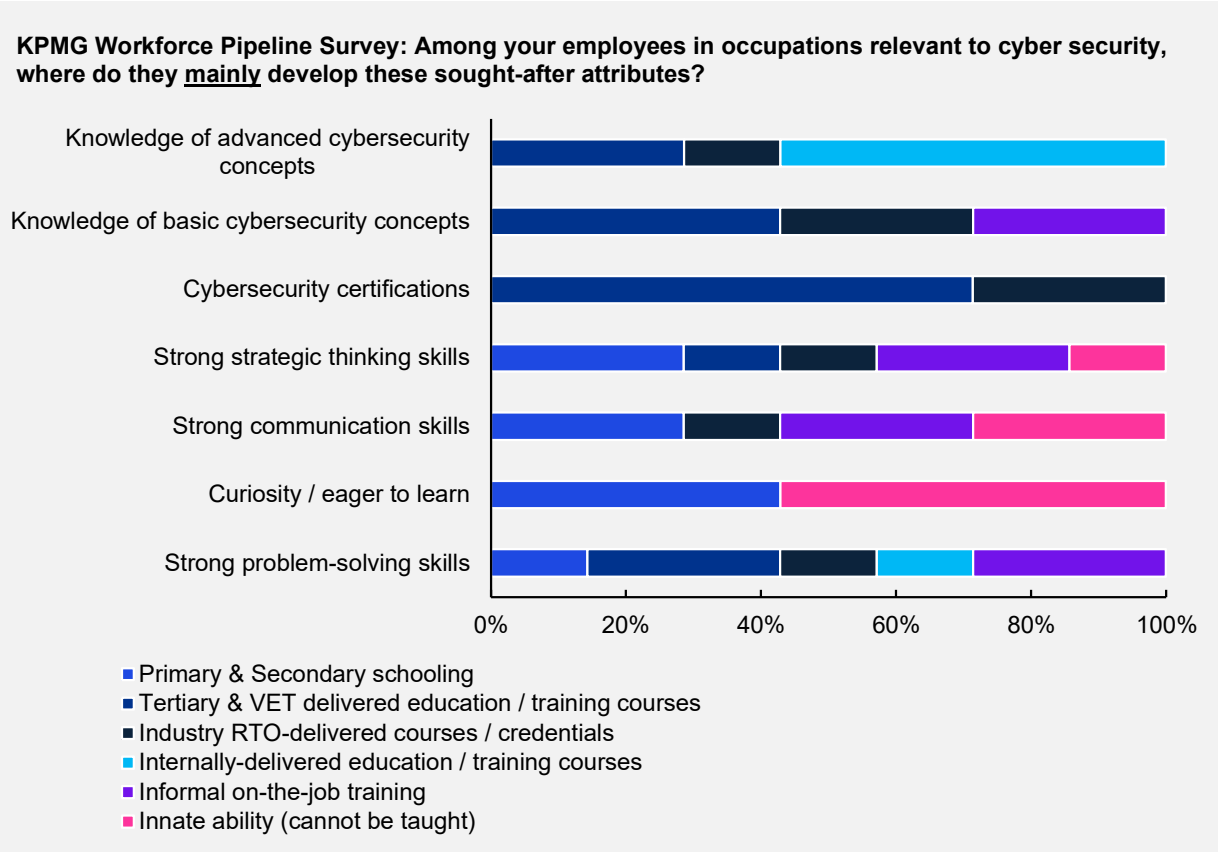


Figure 7: KPMG Cyber Security Industry Workforce Pipeline Survey Question 6: Among your employees in occupations relevant to cyber security, where do they mainly develop these sought-after attributes? (Source: Cyber Security Industry Workforce Pipeline Survey Question 6, 2022, n=7).

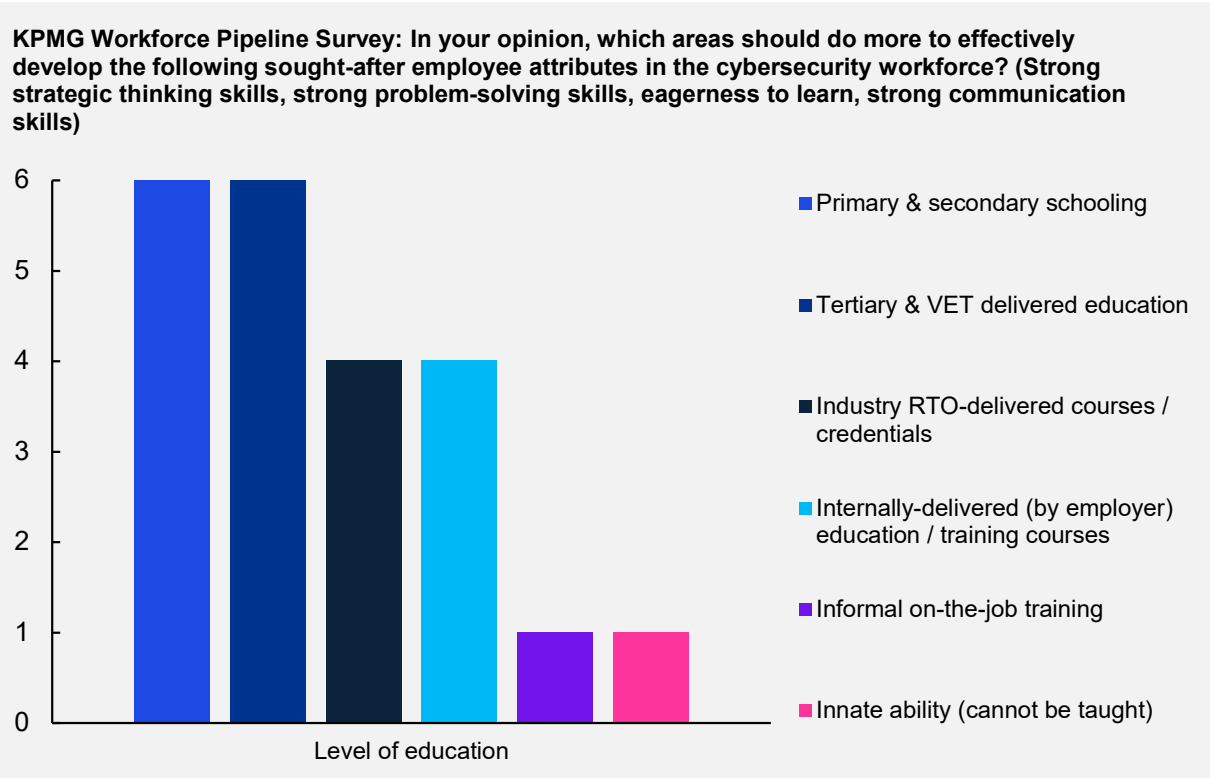


Figure 8: KPMG Cyber Security Industry Workforce Pipeline Survey Question 7: In your opinion, which areas should do more to effectively develop sought-after employee attributes in the cyber security workforce? (Source: KPMG Cyber Security Industry Workforce Pipeline Survey Question 7, 2022, n=7).

Interviews. Interview participants indicated that a significant factor in the challenge for trainers remaining relevant in skills is the speed at which the industry moves. Due to this, there was a view that industry needed to do more to assist in the academic space to ensure that those training cyber security skills are able to provide relevant and modern experience to their students.[57]

10.2.1 The cyber industry is funding and developing their own workforce pipeline initiatives

Interviews. Industry representatives interviewed indicated that they are undertaking a number of initiatives to upskill workers in the post-secondary/traineeship and the continuous education/reskilling spaces. This is detailed in Appendix C (Figure 26). It was noted that the sector could benefit from greater coordination and collaboration as many of these initiatives tend to be ad hoc, or focused on a particular organisation's workforce pipeline rather than the broader sector pipeline.[58]

10.2.2 There is the opportunity for the cyber security industry to collaborate more to address shared problems

Desktop research. The benefits of collaboration:

> *Given the significant consequences of a cyber security breach, many organisations are calling for greater collaboration; the benefits of which include greater intelligence sharing, a cohesive response to threats and robust international infrastructure*.[59]

Encouraging collaboration within the cyber security industry is also a key enabler:

> *It's crucial that private-public partnerships are not only encouraged on a national scale, but globally. Participating in global forums, sharing intelligence and developed global frameworks will inevitably improve cyber-resilience. Finally, co-ordinated global responses may deter nation state attacks, and increase trust between co-operating countries.*[60]

Interviews. Some interview participants shared the view that industry is uniquely placed within the cyber security community to provide support to the vocational industry at large to assist with the challenges in keeping trainers' skills relevant and up to date. Industry representatives indicated that they would be particularly interested in initiatives that support cyber-suitable skills and attributes in primary and secondary schooling, as well as up-skilling and cross-skilling for early and mid-career employees. These reflect closely to the areas in Figure 26 where industry is not currently developing their initiatives. Industry reported that they are particularly interested in initiatives that support cross-skilling that deliver critical skills in emerging technology. There was also an interest amongst industry stakeholders in initiatives which support skills growth in emerging technologies, such as AI, blockchain, quantum computing and machine learning.

Industry is keen to address the cyber security workforce shortage as a means of supporting their own enterprise cyber security operations. Stakeholders consulted indicated that organisations with the greatest interest are also motivated by the economic opportunity in the cyber security services sector and evolving regulatory requirements (e.g. reforms to the *Security of Critical Infrastructure Act 2018*). Despite the acute competition for cyber security talent, industry stakeholders indicated that there is a lot of 'goodwill' within the sector to support initiatives that develop the overall size and quality of the cyber security skills pipeline which they are all dependent on.[61]

[57] Consultation G, Consultation P, Consultation S.
[58] Consultation R.
[59] McGregor Boyall. (2021 June 15). *The importance of cross-sector cybersecurity collaboration*. McGregor Boyall. Retrieved from: https://www.mcgregor-boyall.com/our-thinking-library/2021/06/the-importance-of-cross-sector-cybersecurity-collaboration/260
[60] McGregor Boyall. (2021 June 15). *The importance of cross-sector cybersecurity collaboration*. McGregor Boyall. Retrieved from: https://www.mcgregor-boyall.com/our-thinking-library/2021/06/the-importance-of-cross-sector-cybersecurity-collaboration/260
[61] Consultation B.

10.3 Context: The role of government in addressing the cyber security skills gap

10.3 Key Findings

- The Australian Government has a key role in addressing the cyber security skills gap and in growing the technology workforce at large, particularly to support REDSPICE, AUKUS and CISoNS policies, programs and reforms.
- There are several programs of activity at the Federal, State and Territory government level that seek to address the gap in supply of skilled workers for the digital economy, including but not limited to Cyber Security.
- Primary and secondary schooling curricula plays an important role in fostering learning and thinking attributes that are sought after in the cyber industry.
- Industry generally welcome the support of government collaborating to address cyber workforce skills shortages.

Desktop research. Cyber security is a key strategic and bipartisan interest: successive Australian governments have recognised that Australia's cyber security workforce will need to grow significantly in coming years.[62] Recently the Australian Labor Party (who recently formed government) has committed to delivering 1.2 million tech-related jobs by 2030.[63]

Survey responses. Participants in our Cyber Security Industry Workforce Pipeline Survey indicated that they see the role of Government to be in developing initiatives which focus on developing skills in problem solving, curiosity, communication, strategic thinking and basic and advanced cyber security knowledge and skills, as well as supporting quality assurance of cyber security certifications of the workforce. This is detailed in Figure 6. In addition to this, 52 per cent of participants felt that more should be done to develop workforce skills within Primary & Secondary schooling and Tertiary & Vocational Education and Training (VET) delivered education. This is detailed in Figure 8.

Interviews. The cyber security of Australia's Critical Infrastructure (CI), control systems, IT and operational technology (OT) is critical. Government is interested in the workforce skills and training requirements for maintaining the security of CI, control systems, IT and OT, to support REDSPICE, AUKUS and CISoNS policies, programs and reforms. This was emphasised in interviews with several stakeholders.[64]

Interview participants indicated that it was not clear whether a gap analysis had been undertaken by the Government, during the development of the CSSPIF, to identify what skills are required by or are priorities for industry. This was evidenced by the lack of visible industry consultation during the grant design phase, and the focus of the grant on tertiary and VET education, despite known barriers to entry at earlier education stages.

10.3.1 Government has a key role in supporting the training and employment pathways of the cyber security industry

10.3.1.1 There are several programs of activity at the Federal, State and Territory government level that seek to address the gap in supply of skilled workers for the digital economy, including but not limited to Cyber Security

Desktop research. Similar to industry, government is also investing in traineeships, for example, the Australian Signals Directorate's CyberEXP Program and the Australian Defence Force's Cyber Gap Program are focused on developing Australia's workforce to meet this growing demand.[65] A sample of 37 digital skills initiatives being

[62] MP Price, M. (2021 October 25). *$60m to grow Australia's cyber security workforce*. Retrieved from: https://www.minister.industry.gov.au/ministers/price/media-releases/60m-grow-australias-cyber-security-workforce
[63] Australian Labor Party. 2022. *Media release: Labor's plan for 1.2 million tech jobs by 2030*. Retrieved from: https://www.alp.org.au/policies/growing-tech-jobs#:~:text=An per cent20Albanese per cent20Labor per cent20Government per cent20will,work per cent20in per cent20this per cent20growing per cent20industry.
[64] Consultation D, Consultation E, Consultation R.
[65] AustCyber. 2020. *SCP - Chapter 1 - The Australian cyber security sector today*. Retrieved from: https://www.austcyber.com/resources/sector-competitiveness-plan/chapter1

run at the Federal level can be found on DISR's website, demonstrates both the breadth of initiatives and the number of different departments involved.[66]

Interviews. One stakeholder indicated that a market scan they conducted had identified over 100 different funding opportunities within the digital skills space, including at a Federal and State/Territory level.[67] Despite the volume of initiatives being run to address the digital skills shortage, stakeholders indicated that it was not clear how, if at all, these programs fit together to address the larger issue at a macro level.

Survey responses. This is reflected in survey responses (see Figure 9 below) where 42.9 per cent of respondents disagreed that the role and opportunity presented by the CSSPIF, alongside other federal and state government programs, is clear.

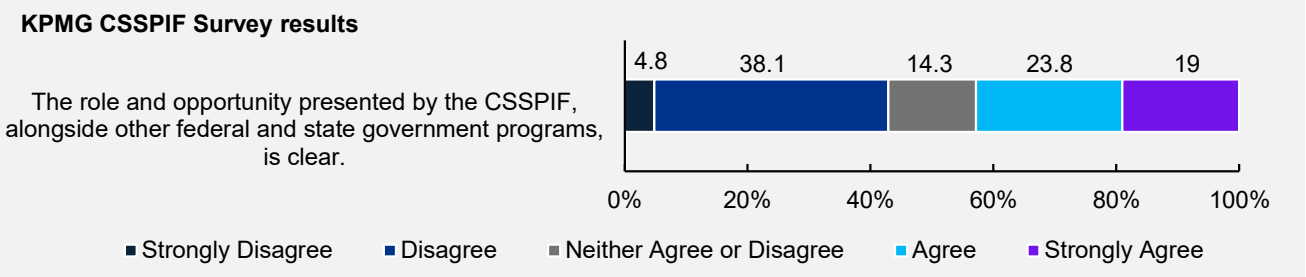


Figure 9: KPMG CSSPIF Survey: The role and opportunity presented by the CSSPIF, alongside other federal and state government programs, is clear (Source: KPMG CSSPIF Survey Question 13, 2022, n=21).

10.3.1.2 Primary and secondary schooling curricula plays an important role in fostering learning and thinking attributes that are sought after in the cyber industry

Interviews. Industry stakeholders interviewed indicated that there is a strong interest for Government to act within Primary and Secondary school curricula to foster the transferrable and desirable skills for cyber security employees. This is reflected in Figure 9 above, where industry stakeholders indicated that there are not currently as many initiatives targeting skills development in this part of the workforce pipeline. This is also reflected in survey responses, shown in and Figure 8 above), where participants indicated that Primary and Secondary schooling is where these skills are primarily developed and that these areas needed to be doing more to develop these skills in students (Figure 7).

10.3.2 Industry generally welcome the support of government collaborating to address cyber workforce skills shortages

Desktop research. The Federal Government has funded several initiatives and organisations to enable collaboration and networking across the Australian cyber community.

The ACSC was developed as a hub for private and public sector collaboration and information-sharing on cyber security to prevent and combat threats and minimise harm to Australians. They provide advice and assistance across the whole economy, including critical infrastructure and systems of national significance, Federal, State, and local governments, small and medium businesses, academia, not-for-profit organisations and the Australian community.

AustCyber was established in 2017 as an independent and not-for-profit organisation funded by Federal Government grants and an important part of *Australia's Cyber Security Strategy 2020*. It enables cyber security research, development, and innovation. Guided by a Board with industry experience, AustCyber aims to ensure its program of activities are underpinned by evidence gained through extensive research and consultation. AustCyber's flagship *Sector Competitiveness Plan* and *Industry Roadmap* outline the opportunity for Australia's cyber security sector to support growth across the whole economy.[68]

Despite the above efforts, governments and private organisations are finding it challenging to find skilled cyber security professionals. Some suggest that to ensure a pipeline of skilled ICT and cyber security professionals,

[66] Department of Industry, Science and Resources. 2022. *Government initiatives*. Department of Industry, Science and Resources. Retrieved from: https://www.industry.gov.au/data-and-publications/australias-tech-future/government-initiatives
[67] Consultation R.
[68] AustCyber. 2022. About Us. *AustCyber*. Retrieved from: https://www.austcyber.com/about-us

it is critical that Australian policy makers, education providers and businesses work together to increase the number of professionals coming into the workforce and increase the common services that can be leveraged.[69]

For its part, AustCyber aims to provide a national layer of coordination on cyber security innovation to multiply and connect people and organisations across Australia, keeping a strategic view across local ecosystems in States and Territories and have formed partnerships with relevant industry associations across the economy to cross-promote industry interests and to support industry to have a voice in government policy development and implementation.[70, 71] AustCyber has also developed 'Friends of AustCyber', which is described as a 'network of innovative, like-minded and future focused companies and organisations that are active in the global cyber security sector and open to all'.[72]

Interviews. Some Participants suggested that a role of government was to help cross-promote the projects and support networking and coordination across the sector.[73] Several stakeholders interviewed indicated that they would be highly interested in participating in a network between recipients of the CSSPIF to share learnings with each other.[74]

10.3.3 Government is a key partner to the industry in regulating the quality of the cyber security education and training system

Desktop research. There is a challenge in balancing the development of nimble and responsive credentials (outside of the Australian Qualifications Framework [AQF]) with quality control mechanisms. Some research has concluded that the current architecture of the VET system is impeding the introduction of the flexible, industry-current, nationally accredited skills training required by employers.[75] One of the major impediments is the current structure of the National Training Packages and the processes by which they are developed. There are concerns among RTOs, industry groups, employer organisations and governments that training packages are too cumbersome and complex, which means qualifications can quickly become out of date.

Interviews. Stakeholder interviews indicated that there are significant challenges in the training provided within the VET sector remaining relevant due to the quality control mechanisms currently in place.[76] However, these mechanisms were also seen as important to retaining the reputation of the quality of Australia's education.

[69] KPMG. (2021 September 30). *Addressing Australia's cyber security challenges and opportunities*. KPMG. Retrieved from: https://home.kpmg/au/en/home/insights/2021/09/australia-cyber-security-challenges-opportunities-kpmg-submission.html
[70] AustCyber. 2022. *Collaborate and coordinate*. AustCyber. Retrieved from: https://www.austcyber.com/grow/collaborate
[71] AustCyber. 2022. *Collaborate and coordinate*. AustCyber. Retrieved from: https://www.austcyber.com/grow/collaborate
[72] AustCyber. 2022. *Collaborate and coordinate*. AustCyber. Retrieved from: https://www.austcyber.com/grow/collaborate
[73] Consultation I, Consultation Q, Consultation R.
[74] Consultation G, Consultation J, Consultation O.
[75] Digital Skills Organisation. 2021. *Towards a new model for the development of digital skills*. pp. 14. Retrieved from: https://digitalskillsorg.com.au/assets/pdf/Digital_Skills_Organisation_Discussion_Paper.pdf
[76] Consultation G, Consultation P, Consultation S.

11 Appendix D – Observations of the CSSPIF Program Logic

11.1 Program Inputs: CSSPIF Program Design

11.1.1 The CSSPIF Guidelines are standard and are comparable to other grants programs, but less experienced applicants need more supportive information

11.1.1 Key Findings

- Guidelines identify objectives and intended outcomes (i.e. to improve the quality or quantity of cyber security professionals, including women).
- The CSSPIF is designed to fund projects to support innovative approaches through collaboration to improve the future cyber security workforce pipeline.
- Guidelines align with Commonwealth Grant Rules and Guidelines with eligibility requirements.

Desktop research. The CSSPIF Guidelines Round 1 and 2, both aimed to improve the future cyber security workforce pipeline by supporting partnerships between industry and education providers, increasing diversity in the cyber security workforce, improving the quality and quantity of cyber security professionals in Australia and funding innovative approaches (see Table 2). Between Rounds 1 and 2, the Department altered the Guidelines to expand the focus of the CSSPIF to other underrepresented groups (namely, Indigenous Australia, regional and remote based workers, and neuro diverse individuals), and to limit the eligibility of lead applicants to non-government organisations. The CSSPIF Grant Guidelines' eligibility requirements align with the Commonwealth Grant Rules and Guidelines. As demonstrated in Table 7 below, the objectives and intended outcomes of the grant funding guidelines were refined between the two rounds.

Table 7: Comparison of objectives and intended outcomes between CSSPIF Rounds 1 and 2.

	Round 1	Round 2
Objectives	• Improve the quality and quantity of cyber security professionals in Australia, including increasing the participation of women in cyber security; • Improve collaboration between industry and the education sector to build the quality and availability of cyber security professionals in Australia; and • Support industry and academia to build Australia's future pipeline of skilled cyber security professionals.	• Increase diversity in the cyber security workforce; • The creation of new and innovative ways to improve the quality and quantity of cyber security professionals in Australia; and • Improve collaboration between industry and the education sector to build the quality and availability of cyber security professionals in Australia support industry and academia to attract, train and place cyber security talents into their businesses.

	Round 1	Round 2
Intended Outcomes	• Increased availability of cyber security professionals in Australia; • Increased quality of cyber security professionals in Australia; • Increased participation of women in cyber security professions; • Innovative or new ways to improve cyber security skills; and • Stronger partnerships between industry and education providers to enhance cyber security related skills.	• Increased diversity of the cyber security workforce including lifting the participation of women, Indigenous Australia, regional and remote based workers, and neuro diverse individuals; • Delivering a pipeline of highly skilled cyber security professionals to meet the current and future need of Australia's digital economy; and • Enhanced Australian sovereign cyber security capability to underpin our growing digital economy and the safety of all Australians.

Interviews. Stakeholders that are familiar with the grants process indicated that the CSSPIF Grant Guidelines were similar to grants programs that they have previously experienced and the CSSPIF Grant Guidelines and processes are robust and necessary.[77] Stakeholders expressed that this standard process may be onerous for organisations that are new to the application process and that they may require more support and assistance to complete an application to the Department's standards. Stakeholders indicated that it may be beneficial host a webinar, when the application process is open, to allow for the intended audience to engage with the Department directly.[78] Stakeholders referred to the Boosting Female Founders Round 2 Webinar as a 'best practice' example.[79]

11.1.2 The Program's design is broad and inclusive in scope, but some needs of Industry and disadvantaged groups are not met by projects funded to date

11.1.2 Key Findings

- There was limited evidence that the Department undertook a gap analysis or research to understand the nature and magnitude of the problem.
- Some interview participants expressed the sentiment that the problem is bigger than the fund can address.
- Unclear of the extent to which the intended audience (industry & underrepresented groups) were consulted & participated in co-design of the Program.
- The guidelines intended to increase diversity in the cyber security workforce, however, there was no evidence that peak bodies and representatives of the cohorts were engaged during the development of the guidelines.

Desktop research. The CSSPIF aims to support projects which can help to grow a skilled workforce. It is part of the Cyber Security National Workforce Growth Program which is an element of *Australia's Cyber Security Strategy 2020.*[80]

Eligible activities to be funded through the CSSPIF must be aimed at improving the availability, quality or pipeline of skilled cyber security professionals by enhancing partnerships between industry, employers, schools and tertiary providers. Activities may include innovative new projects such as:

- Developing and delivering specialist cyber security courses for professionals,
- Retraining initiatives to help existing professionals in other disciplines transition to cyber security roles,
- Establishing cyber labs, training facilities, cyber simulators,
- Training or professional development for teachers and board executives, including through practical partnerships or exchanges with industry,
- Establishing student delivered cyber security services,

[77] Consultation G, Consultation J, Consultation M, Consultation O, Consultation Q.
[78] Consultation G, Consultation H, Consultation K, Consultation N.
[79] Consultation H, Consultation K.
[80] Department of Home Affairs. 2020. *Australia's Cyber Security Strategy 2020*. pp. 8. Retrieved from: https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

- Establishing new scholarships (where at least 50 per cent of your scholarships will be reserved for women, or to improve diversity of workforce),
- Establishing new apprenticeships, or apprenticeship-style courses in higher education,
- Establishing new internships, cadetships, work experience and staff exchanges, and
- Any other innovative ideas to meet the cyber security needs of businesses may also approved.[81]

There was limited documentary evidence available of the Department's gap analysis research into the nature and magnitude of the problem that the CSSPIF aimed to address. This comes back to the question of why the intention was to have a broad program that might chip away at some elements of the problem over having a purposefully targeted program trying to focus efforts on a small number of priorities.

There are existing organisations that undertake activities to gain an understanding of industry needs, for example AustCyber aims to ensure its program of activities are underpinned by evidence gained through extensive research and consultation. It was reflected in AustCyber's *Sector Competitiveness Plan 2019* that:

> *Australia's core cyber security workforce is growing strongly, but not sufficiently to fill the substantial short-term demand for cyber security professionals […] while government, industry and educational institutions have all undertaken a range of initiatives to strengthen workforce growth, the inevitable delay in any skills system means that the impact of these efforts is yet to be fully realised*.[82]

Interviews. Stakeholders expressed the sentiment that the problem is bigger than the fund can address. Government stakeholders noted that that the skills shortage is still not close to having been addressed and that there is a need to target the Program to a specific industry need, such as to include cyber skills at the secondary and post-secondary level for all industries.[83] [84] Others noted that they were not aware of research undertaken by the Government for where and what skills were required during the design of the CSSPIF.[85] Stakeholders expressed that a gap analysis would be beneficial and would support the Department to tailor the grant guidelines to the needs of industry.[86]

Stakeholders indicated that they have an ongoing relationship with the Department. Through this, the Department could gain a high-level understanding of the key activities that key stakeholders are undertaking. However, one stakeholder expressed that that there was a lack of visible and formal consultation with industry in the initial design of the grant program.[87] As such, there was a lack of understanding of specific industry needs and the barriers or points of friction prior to guidelines being published, namely the co-contribution requirement (described in section 11.1.4). Additionally, stakeholders queried as to whether peak bodies and representatives of underrepresented cohorts were consulted on the revised Round 2 Guidelines, considering the revised Guidelines' objective to increase diversity in the cyber security workforce.[88] The evaluation found that it was not clear if the Department understood how these cohorts interacted with the cyber security sector and the best ways to involve and engage the cohorts in a meaningful way. Section 10.1.6 explores the segments of Australian society are underrepresented in the cyber security workforce.

Survey responses. Survey respondents also agreed (n=21, 80.8 per cent) with the sentiment the CSSPIF should be targeted to specific areas of need in the workforce. Survey respondents agreed (n=21, 66.6 per cent) that changes are required to the Program to increase uptake of the Program across the sector. As shown in Figure 11, stakeholder opinion is mixed as to whether the CSSPIF's design is conducive to increasing participation of neuro-diverse, Indigenous Australians and women in cyber security.

[81] CSSPIF Round 1 Guidelines, CSSPIF Round 2 Guidelines.
[82] AustCyber. 2019. *Australia's Cyber Security Sector Competitiveness Plan 2019. Chapter 3*. Retrieved from: https://www.austcyber.com/resources/sector-competitiveness-plan-2019/chapter3
[83] Consultation S.
[84] Consultation Q.
[85] Consultation C.
[86] Consultation C, Consultation I, Consultation P.
[87] Consultation P.
[88] Consultation C.

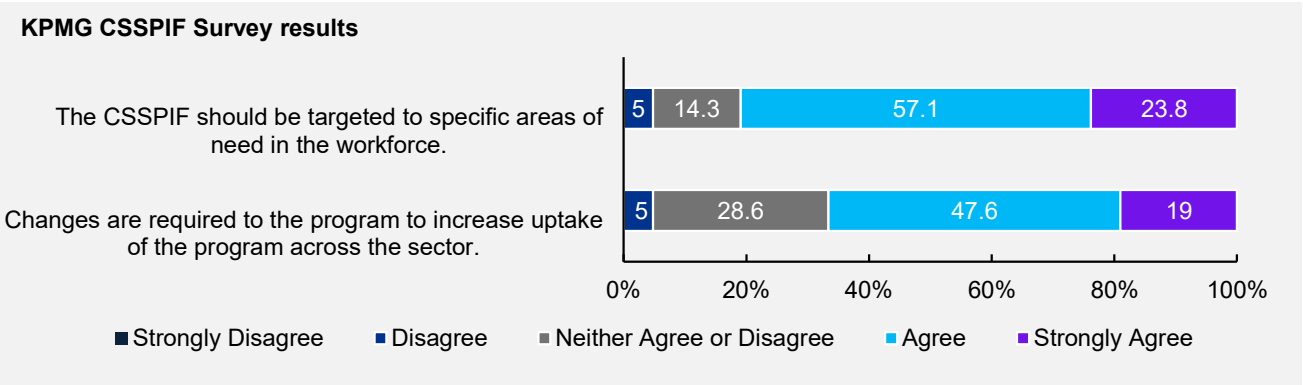


Figure 10: KPMG CSSPIF Survey, question 5 and 24: CSSPIF Design (Source: KPMG CSSPIF Survey Question 5 and 24, 2022, n=21).

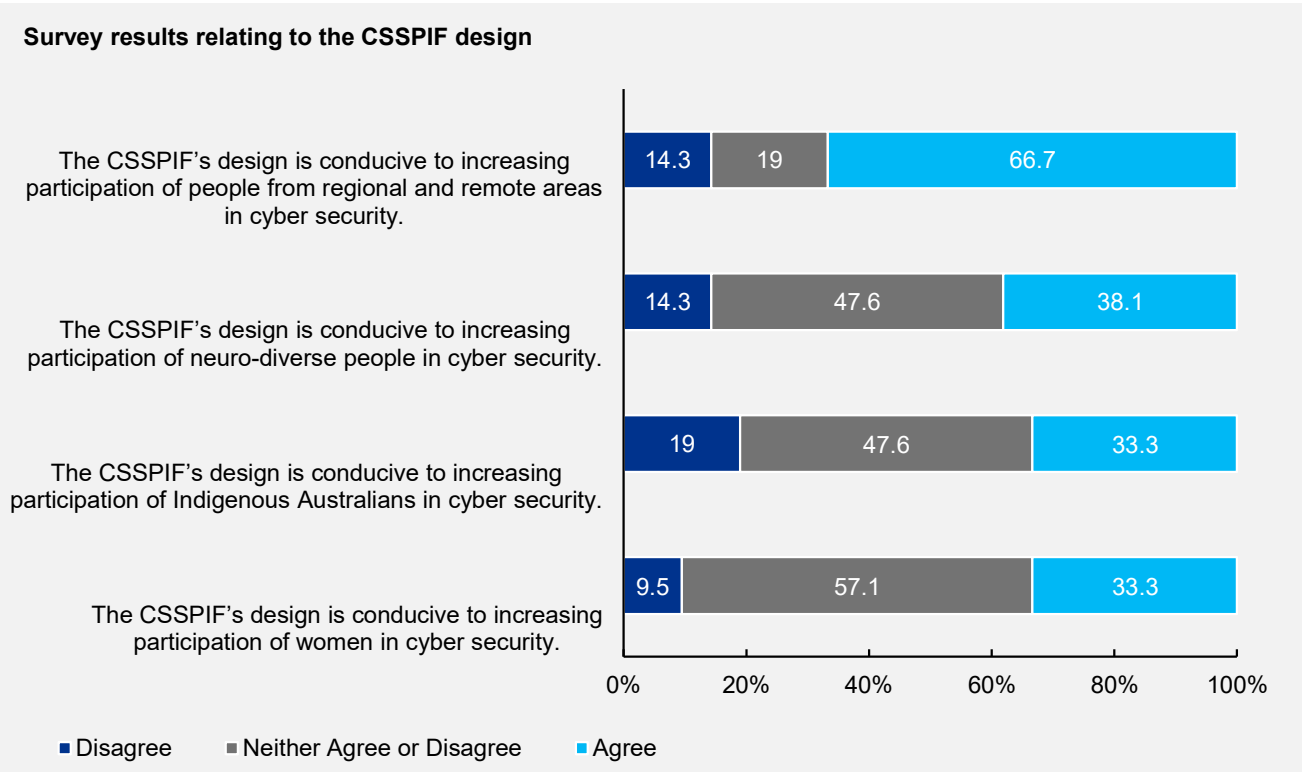


Figure 11: Survey results relating to CSSPIF design (Source: KPMG CSSPIF Survey, 2022, n=21).

11.1.3 The Program's design suits a target audience of bigger, better-resourced and more experienced applicants

11.1.3 Key Findings

- The CSSPIF targeted the cyber security industry and the education sector, at large, rather than identifying and targeting a specific niche audience within the sector.
- Some interviewees expressed the sentiment that providing Government grants to entities that are experienced in the Grants process is unlikely to shift the dial or deliver a step change in the cyber skills industry.

Desktop research. As mentioned in the Guidelines' objectives and intended outcomes (see Table 2), the CSSPIF aimed to improve collaboration between industry and the education sector. The CSSPIF Round 1 and 2 Guidelines appeared to target to the cyber security industry and the education sector, at large. The vast majority (88 per cent) of Australian cyber security providers were organisations with less than 100 employees, as shown in Figure 12. The evaluation found limited evidence to suggest that the Department had scoped the

attributes of cyber security industry firms during the development of the Round 1 and Round 2 Guidelines. Section 11.1.4.2 further explores how the CSSPIF's financial requirements hindered the participation of smaller firms, and – in so doing – limiting the participation of the majority of the cyber security sector.

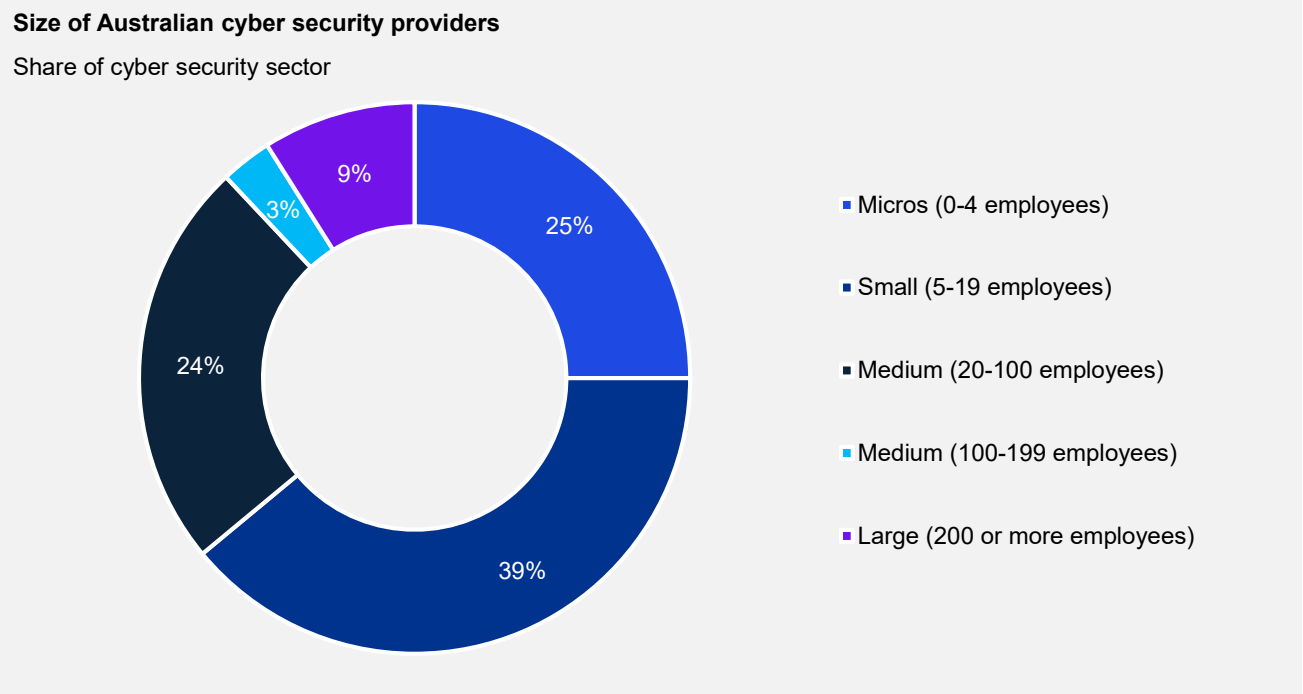


Figure 12: Size of Australian cyber security providers (Source: adapted from AustCyber Australia's Cyber Security sector competitiveness Plan – 2020 Update [89]).

Interviews. As discussed in above in section 11.1.2, a gap analysis was not undertaken to determine the cyber security industry's need, thus the CSSPIF was not tailored to a specific niche audience within the sector. Some stakeholders agreed that this may have resulted in a broader range of application types, increasing innovation in applications. Other stakeholders noted that targeting the cyber security industry and education sector at large may have meant that potential applicants were not reached by CSSPIF awareness communications. CSSPIF communications are discussed further in section 11.2.2.

Some interviewees expressed the sentiment that grants programs are targeted toward entities that are experienced in the Grants process and this is unlikely to shift the dial or deliver a step change in the cyber skills industry.[90] Stakeholders noted that the main reason for this perception is that the standard Grants process is onerous and is difficult to navigate, for organisations that are not experienced with participating in Grants programs.[91] Many stakeholders agreed that the application process should remain robust to mitigate risk.[92] However, it was suggested that the Department provide more support for potential applicants during the application process to assist them to navigate the process, communication management.[93] This is further discussed in section 11.2.3. Some stakeholders expressed that by targeting towards entities that are experience in the Grants process, it could potentially lead to the same outcomes.[94] However, others suggested that it may continue to drive innovation and support a growing cyber security workforce, regardless of whether applicants were experienced in the Grants process or not.

[89] AustCyber. 2020. *Australia's Cyber Security Sector Competitiveness Plan 2020 Update*. pp. 17. Retrieved from: https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2020
[90] Consultation C, Consultation F.
[91] Consultation D, Consultation F.
[92] Consultation F, Consultation G.
[93] Consultation D, Consultation F.
[94] Consultation C, Consultation F.

11.1.4 Guideline Requirements

11.1.4 Key Findings

- Guidelines stipulate project partners must be industry, education or government.
- Stakeholders believe that collaborative partnerships require formal arrangements to be in place.
- Financial requirements present a barrier to potential applicants.
- Reviewing the fixed co-funding requirement may encourage smaller entities to participate
- Co-contribution of at least $250,000 and $500,000 in liquid assets are key distinguishing design features to increase investment and demonstrate applicant commitment.

11.1.4.1 The Program's partnership requirements incentivise collaboration

Desktop research. The CSSPIF Round 1 and Round 2 Guidelines state that:

> *Each application must be a joint application with a lead organisation, who is the main driver of the project and is eligible to apply, and at least one other project partner.*[95]

The CSSPIF Round 1 and 2 Guidelines also state that:

> *For the purposes of this grant opportunity, partnership refers to collaboration between organisations towards shared goals. Applicants are not required to set up formal business partnership structures for the program.*[96]

Partners are required to be an industry organisation, within the education sector or government. This aligns with the CSSPIF's objective to improve collaboration between industry and the education sector. Further, Round 1 Guidelines allow for the lead applicant to be an organisation within the education sector, industry or government. Whereas Round 2 Guidelines state that a state, territory or local government department is not eligible as the lead applicant to drive industry and education organisations to assume a larger role in proposed projects.

Interviews. Stakeholders indicated that the partnership requirement incentivised organisations to form new partnerships that would not have formed if the CSSPIF did not exist. As such, stakeholders expressed the sentiment that the partnership requirement has benefitted singular organisations and the cyber security workforce, at large. For detail on the partnerships formed as a part of the CSSPIF, see Appendix F.

Although a formal arrangement was not a requirement of the Guidelines, stakeholders expressed that formal arrangements were preferred, by the participating organisations, to provide them with assurance. Some stakeholders noted that the timeframe in which applications were open was not sufficient for organisations to build relationships with potential partners and execute formal arrangements.[97] Thus, deterring potential applicants from submitting an application. Conversely, one successful applicant noted that they already had existing relationships with partnering organisations, so the partnership requirement was not an issue for them.[98]

11.1.4.2 The Program's financial requirements mitigate some risks, but may hinder participation from smaller, innovative potential applicants

Desktop research. The CSSPIF Round 1 and 2 Guidelines state that:

- *The grant amount will be up to 50 per cent of total eligible project expenditure,*
- *The minimum grant amount is $250,000,*
- *The maximum grant amount is $3 million, and*
- *To be eligible got the program, the applicant must have at least $500,000 in eligible expenditure.*[99]

As mentioned in section 11.1.3, the vast majority of cyber security providers are SMEs, thus, the financial requirement risks excluding a significant proportion of the intended audience of the CSSPIF.

[95] CSSPIF Round 1 Guidelines, CSSPIF Round 2 Guidelines.
[96] CSSPIF Round 1 Guidelines, CSSPIF Round 2 Guidelines.
[97] Consultation F, Consultation N.
[98] Consultation M.
[99] CSSPIF Round 1 Guidelines, CSSPIF Round 2 Guidelines.

Interviews. Stakeholders indicated that the co-contribution minimum value of $250,000 may have hindered SMEs and more regional organisations from applying, as these organisations are unlikely to make the funds available within the CSSPIF program period.[100] The requirement for an applicant to have at least $500,000 in eligible expenditure added additional concern to SMEs, also deterring them from applying. Stakeholders suggested that lower award of grant amounts (i.e. below $50,000) as a way to reduce barriers to participation for SMEs with less access to investment capital for the financial co-contribution.[101]

Stakeholders also noted that the co-contribution requirement increased applicant investment and demonstrated applicant commitment, resulting in a higher quality of applications and filtering out projects that were not viable. To ensure a high quality of applications remain and enable SMEs to apply, stakeholders suggested that an alternative risk-based approach to co-contributions be considered by the Department, such as that the Department accept gifts in kind or other measures of viability (i.e. a strong evidence base to show that the project is viable and will achieve its outcomes).[102] One stakeholder suggested that the Department hold open grant rounds, referring to the Department of Foreign Affairs and Trade's (DFAT's) Australia's Cyber and Critical Tech Cooperation Program as an example, to allow time for potential applicants to make the significant funds, that the Program requires, available and form partnerships, as well as support innovation.[103]

11.2 Program Activities: CSSPIF program delivery and implementation

11.2.1 Communications planning has improved over time, but more can be done to clarify internal roles, inputs, timeframes and expectations

11.2.1 Key Findings

- The approach and use of communications has been moderately effective, but has improved since Round 1.
- Earlier engagement and clearer expectations between the policy, communications, program design and contract management teams internal to the Department can improve program promotion and sector engagement.

Desktop research. A review of program documentation and online media revealed a limited degree of program cross promotion generally and opportunities exist to improve program awareness across a number of Australian Government and Departmental sites and publications. For example, despite a media release identifying the eight successful recipients of Round 1, there are no links to current information in relation to the organisations and projects funded under the Program, or training opportunities being created.[104] There may be opportunity to update communication plans to better articulate internal roles and responsibilities and better enable the promotion of projects government has funded to a wider audience during the life of the project.

Interviews. Stakeholder consultation with the Department revealed that the approach to program communications and promotion differed between CSSPIF grant funding Rounds 1 and 2. There was no dedicated team to manage the promotion for Round 1. However, a communications plan was developed for Round 2 with the Department's communications and media team engaged to support the Program.[105]

Improvement in communications activities between Rounds 1 and 2 was confirmed by two internal stakeholders.[106] Despite this improvement, it was also noted that the expectations between teams internal to the Department involved in the CSSPIF program implementation – including policy, communications and contract management staff – could have been clearer. For example, greater support for Regional Outreach Officers to actively promote the Program across networks in regional areas and longer lead times for detailed

[100] Consultation F, Consultation H.
[101] Consultation F, Consultation M, Consultation O, Consultation S.
[102] Consultation D, Consultation F.
[103] Consultation D.
[104] MP Porter, C. (2021 June 29). *Growing the next generation of Australia's cyber security experts*. Australian Government. Retrieved from: https://www.minister.industry.gov.au/ministers/porter/media-releases/growing-next-generation-australias-cyber-security-experts;
[105] Consultation K.
[106] Consultation H, Consultation K.

communications planning was identified as potential avenues for improving program promotion efforts in future.[107]

11.2.2 Effective funding round promotion requires planning and input from the target audiences of the Program

11.2.2 Key Findings

- The CSSPIF rounds were promoted through the Department's website and social media channels, as well as during cyber week and through the Department's networks.
- Program delivery and implementation of efforts to promote and communicate the Program missed key opportunities to reach audiences who may be interested in the grant opportunities.
- Industry participants found out about the CSSPIF through their networks, rather than from the Department's intended communications channels.
- It is unclear who the CSSPIF promotional materials reached due to a lack of available data (e.g. analytics of number of people who clicked on the promotional links).

Desktop research. Rounds 1 and 2 of the CSSPIF was promoted through a number of online channels by the Department, the education sector and media outlets. The Department publicly promoted via the Department's website and social media channels (e.g. LinkedIn, Twitter and Facebook). Furthermore, organisations within the education sector posted articles on their webpages announcing that the CSSPIF rounds were open for applications and providing a brief description of the CSSPIF. Media outlets that targeted the industry also published articles outlining the CSSPIF rounds on their public facing websites. Despite these efforts analytics data is not collected or made readily available (i.e. number of people who clicked on the promotional links) making it unclear who the CSSPIF promotional materials reached.

In addition to the public promotion of the CSSPIF grant funding round, the Department reached out to its networks with the intention of raising awareness of the CSSPIF to the Department's networks and beyond. The Department notes that they requested for the Cyber Security Cooperative Research Centre (Cyber CRC), AustCyber, the Department of Education and the Department of Employment and Workplace Relations (formerly the Department of Education, Skills and Employment), National Security College (NSC), DSO, the Home Affairs, the Royal Melbourne Institute of Technology (RMIT), Regional Managers, the Skills Commission, ITIC Systems, ACSC, Australian Institute of Company Directors (AICD), Australian Information Security Association (AISA), and CISOlens to share the Program with their network (see Table 3).

Interviews. Stakeholders noted that more planning input from the target audience is a potential avenue for improving communications. For example, target audience input on communication content, timing, medium and communication channel preferences may be used to support and improve communication reach.[108] It was also noted that while the CSSPIF program was announced through public channels, it was unlikely that they would have been aware of the Program unless they intentionally went looking for a grant opportunity.[109] The stakeholders that did interact with the CSSPIF promotion through public channels advised through the survey that the CSSPIF communications were accessible and user friendly.

One stakeholder indicated that the Department's attempts to communicate the CSSPIF to their networks (see Table 3) via email, may have reached the wrong contact, hindering their ability to appropriately promote the program.[110] Others revealed that it was not clear to them that the Department had the intention for them to further promote the Program to their networks, meaning that some stakeholders were unaware that there were expectations for them to actively promote the CSSPIF.[111] This echoes a similar experience engaging the Regional Outreach Officers (see section 11.2.1). Thus, the Program may have missed key opportunities to reach audiences who may have been interested in the CSSPIF grant opportunities.

Stakeholders that were familiar with grants processes and looking for grant opportunities indicated that they were made aware of the CSSPIF through the Department's online channels.[112] Whereas stakeholders that may

[107] Consultation H, Consultation K.
[108] Consultation K.
[109] Consultation N.
[110] Consultation N.
[111] Consultation H, Consultation N.
[112] Consultation J, Consultation Q.

have not gone through a grant application process before or were not looking for a grant opportunity indicated that they found out about the CSSPIF through their networks, rather than from the Department's intended communications channels.

Table 8: Departmental CSSPIF Round 1 and 2 promotional activities (Source: stakeholder consultation).

	Round 1	Round 2
Internal activities	• N/A	• Communications plan
Promotions	• Media release • DISR internal promotion	• Media Release • BGA Newsletter (multiple) • JCSC Briefing
Requests for sharing	• CSCRC • AustCyber • DESE • NSC • CSO • Home Affairs • RMIT • Regional Managers	• Home Affairs • ITIC • Skills Commission • Department of Employment and Workplace Relations • ACSC • AICD • ASIA • CISOlens • Regional Managers

Social media	• LinkedIn
	• Twitter
		• LinkedIn
		  ○ Initial post with 19 shares (incl. 8 industry bodies/government agencies,
		  ○ Follow up post with 4 shares (no industry bodies),
		  ○ Closing soon post with 8 shares (incl. ACSC and DTA).
		• Twitter
		• Facebook

Table 9: List of stakeholder suggestions for future promotional activities (Source: stakeholder consultation).

Stakeholder suggestions for best practice program promotion activities

• **Perform a comprehensive market scan to identify the target audience of the program**. Understanding the target audience, and their preferred communication channels and messaging, supports better reach and engagement.
• **Policy and Program Design teams should engage with the Communications and Regional Outreach teams as far in advance as possible**. This will allow for communications content to be designed to:
  ○ Resonate with the intended audience;
  ○ Build awareness prior to applications opening; and
  ○ Provide case studies of previous applications/projects with lessons learnt.
• **Run program guideline co-design workshops with target the target audience of the program.** This will provide a better understand of applicants' capability and expectations to improve program design
• **Launch program and funding rounds during a major event.** Announcements coinciding with a major event relevant to the target audience and the program subject tends to increase program visibility, coverage and impact among the target audience.
• **Ministerial announcements and endorsements add credibility to programs**. Aligning program announcements to external events that are a public opportunity for the minister can support schedules.
• **Allocate a budget for paid program advertisement options**. Paid advertising provides significant benefits, especially when targeting a niche audience not directly covered by existing channels.
• **Run multiple information sharing workshops**. Such workshops should be supported by panel Q&A discussions featuring assessment committee members and previous grant recipients. This interactive engagement helps to:
  ○ Build awareness of the program prior to launch (launch dates not required to be specified);

Stakeholder suggestions for best practice program promotion activities

- Provide further detail of the application process;
- Provide context and understanding of eligibility criteria;
- Develop applicant understanding of application expectations and details; and
- Share learnings from previous applications and projects.

- **Create opportunities to support the cross-promotion of projects funded through the grants program**. This will support the reach and impact of the projects, and networking among grant recipients that can mutually reinforce the objectives of the program.
- **Start developing the communications approach to the next round as soon as a prior round has concluded.** This should build on lessons learned from the round that has concluded.
- **After rounds are completed, collect materials to develop case studies for use in future program promotions.**

11.2.3 Program communication activities post-funding round are limited, but are an opportunity to nurture knowledge sharing between funded projects

11.2.3 Key Findings

- Potential applicants tend to seek advice from trusted entities beyond the Department about the program application process
- Webinars were pointed to as an effective way to engage with potential applicants.
- Once grant applications were assessed and awarded, post-round communications are limited.
- Program delivery and implementation of efforts to foster connections between grant recipients so they can share knowledge as an alumni network.

Interviews. Departmental stakeholders indicated that they are open to and often address potential applicants' queries and clarifications relating the grant guidelines and applicant eligibility, through the AusIndustry team. When potential applicants request AusIndustry's advice, the advice is made publicly available to ensure equitability and that all potential applicants have access to the same information.[113]

Stakeholders observed that potential applicants tended to seek advice about the grant process and guidelines from trusted entities beyond the Department, notably AustCyber. This is evident in Round 2, with AustCyber leading one project and partnering four projects, a full mapping of Program partnerships can be found at Appendix 13. Stakeholders suggested that webinars may be an effective way to engage potential applicants by answering their questions and providing them with advice directly from the Department, they indicated that this has been effective approach for other similar programs, such as ASD's IRAP Program.[114]

Once grant applications were assessed and awarded, the evaluation found that post-round communications were limited. Grant recipients indicated that they do not have the opportunity contact and connect with other grant recipients.[115] Recipients noted that it would be beneficial to connect with other recipients, as some projects are complementary to each other and cross-promotion of project could occur. They also noted that it would give them an opportunity to share lessons learned and knowledge to build an alumni network and a like-minded community.

[113] Consultation D.
[114] Consultation G, Consultation H, Consultation K, Consultation N.
[115] Consultation G, Consultation M, Consultation O.

11.3 Program Activities: CSSPIF applications and funding round decisions

11.3.1 The CSSPIF application process is standard, but poses time and financial barriers for some applicants

11.3.1 Key Findings

- User experiences in relation to guidelines and application process was mixed. However, participants reported that they found the application process to be standard and similar to other government grant application processes.
- Satisfying the current program guidelines is more achievable for applicants that are larger, more established, have access to more resources and are better connected within the cyber security and education/training sectors.
- Potential applicants that are not familiar with government grant application processes require support to meet the Department's requirements.
- Short application timeframes were a deterrent for organisations due to the difficulty to organise partnership arrangements and gain board, Chief Executive Officer (CEO) or equivalent approval within the timeframe that grant rounds were open. Co-contribution requirements also deterred some SMEs from submitting an application.

Interviews. Stakeholders reported that user experiences in relation to the CSSPIF application processes were mixed. Applicants that were familiar with government grant and procurement processes noted that they found the application process to be standard in relation to other government grant application processes.[116] Stakeholders were also of the belief that the grant application processes should remain extensive and robust to ensure government funds are spent in an appropriate manner.[117] As such, stakeholders also expressed that the grant application process can be difficult and onerous for entities that are not familiar with grant application processes. Such entities require support from the Department to navigate the grant application process to ensure support for them to produce high quality applications that meet the Department's requirements.[118]

The evaluation found that entities that were not familiar with grants applications processes were generally SMEs. Stakeholders indicated that SMEs tended to seek CSSPIF application process advice from other entities that were familiar with the processes, such as AustCyber.

Stakeholders indicated that SME applicants experienced difficulties with the application process due to:

- Short application timeframes, which were a deterrent for organisations due to the difficulty to organise partnership arrangements within the timeframe that grant rounds were open; and
- The minimum co-contribution requirement ($250,000) and minimum eligible total project expenditure requirement ($500,000), due to difficulties in designing a project that suited the timeframe and to have the funds readily available.

On the other hand, larger organisations did not express sentiment that these factors were an issue and reported positive experiences with the application process. However, larger organisations noted that the Guideline requirement for the organisations to provide "*evidence of support from the board, CEO or equivalent*" was an area of difficulty.[119] This was due to challenges experienced relating to seeking and gaining board, CEO or equivalent approval within the timeframe that grant applications were open.[120] Stakeholders from larger organisations also expressed that their proposed project spend would not usually require board, CEO or equivalent approval. One stakeholder highlighted that '[seeking] CEO sign-off requirement was significantly difficult for a project of this size'. Thus, seeking and gaining board, CEO or equivalent approval did not appear to be necessary for organisations of all sizes.

[116] Consultation G, Consultation J, Consultation M, Consultation O, Consultation Q.
[117] Consolation F, Consultation N.
[118] Consultation D, Consultation F.
[119] CSSPIF Round 1 Guidelines, CSSPIF Round 2 Guidelines.
[120] Consultation M.

11.3.2 Applicant engagement has been mixed: application quantities reduced while co-contributions grew over time

11.3.2 Key Findings

- Despite the Program being implemented during COVID-19 lockdowns, the CSSPIF attracted a total of 97 applications across two funding rounds which have attracted $55.1M in co-contribution funding from industry.
- Round 1 (57 applications) of the CSSPIF saw higher applicant engagement than Round 2 (40 applications).

Desktop review. The evaluation found that applicant engagement with the CSSPIF in Round 1 exceeded the Department's expectations, evidenced by the 55 applicants that submitted a total of 57 applications (note: two applicants submitted two applications each). In comparison, Round 2 saw the submission of only 40 applicants, of these applicants 12 had submitted applications in Round 1 (see Figure 13). This was a significant drop from the first round, despite the larger amount of funding that was available.

Despite the Program being implemented during 2020-21 COVID-19 lockdowns, the CSSPIF attracted 97 applications from 83 applicants across two funding rounds which have raised $55.1M in co-contribution funding from industry. The overall engagement and investment from industry and the education sector with the CSSPIF to date has demonstrated that the CSSPIF is addressing the cyber security industry's need and/or interest at large.

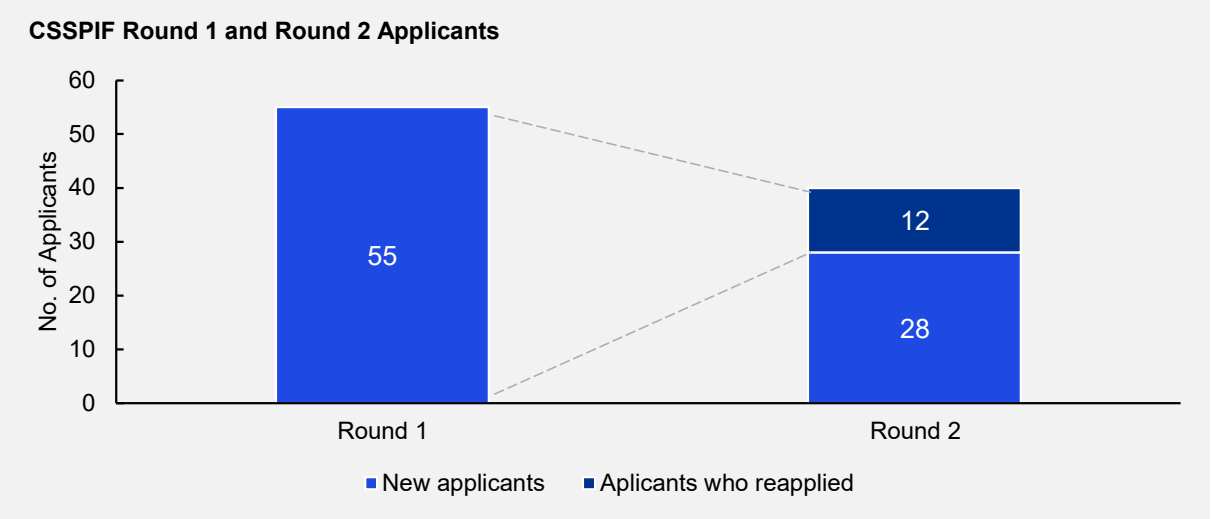


Figure 13: CSSPIF Round 1 and Round 2 Applicants (Source: CSSPIF Round 1 and Round 2 grant applications).

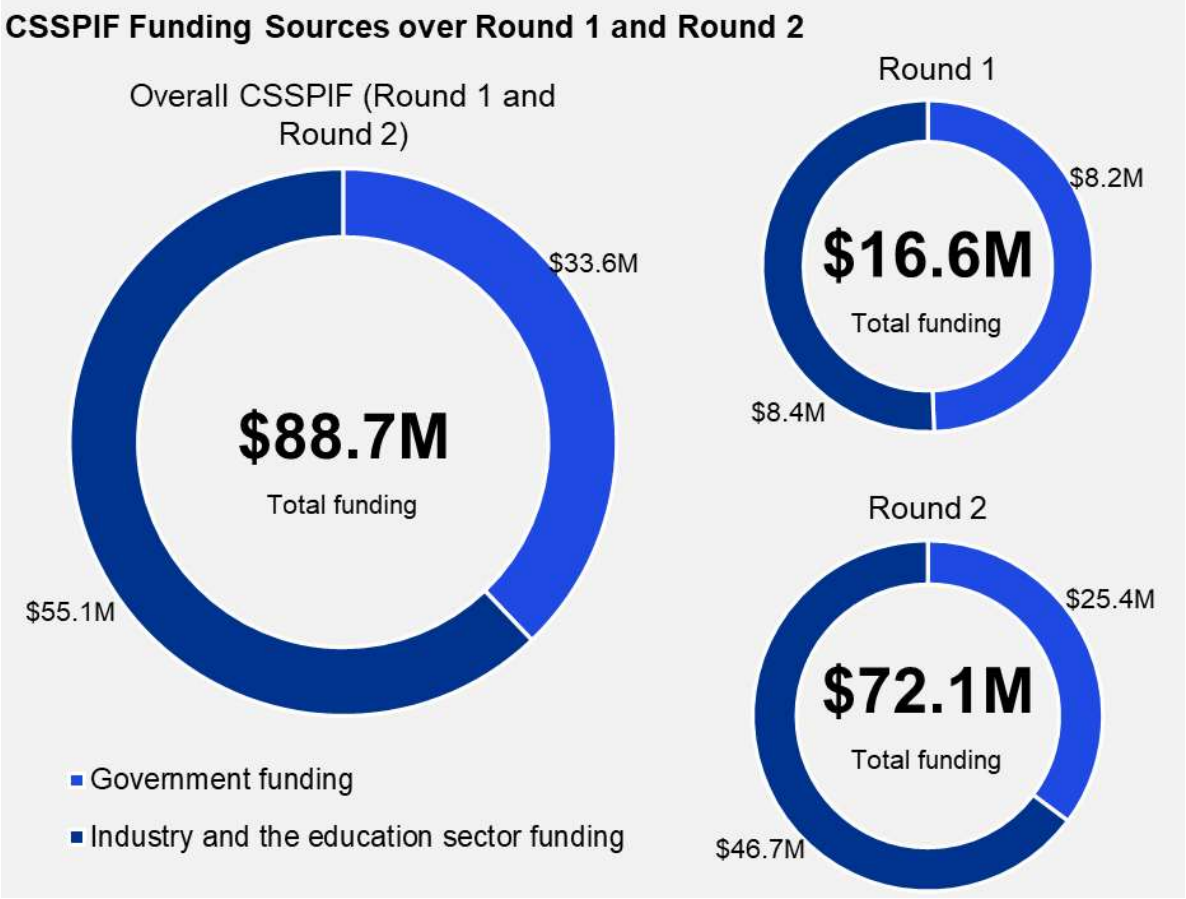


Figure 14: CSSPIF project funding sources over Round 1 and Round 2 (Source: CSSPIF Round 1 and Round 2 grant applications).

Interviews. One stakeholder expressed that the drop in applications may have been due to applicants' potential displeasure from being unsuccessful in Round 1 or due to potential saturation of the intended audience.[121] As mentioned in sections 11.1.2 and 11.2.2, other reasons for the drop in applicants may be due to reasons relating to:

- A lack of understanding of the nature and magnitude of the problem and intended audience when developing the guidelines.
- The communications approach, program delivery and implementation of efforts to promote and communicate the Program missed key opportunities to reach audiences who may be interested in the grant opportunities.

[121] Consultation N.

11.3.3 Most applications received were deemed to be suitable, indicating moderate-to-higher average quality

11.3.3 Key Findings

- Round 1 received a greater volume of 'suitable quality' applications than Round 2.
- Applications for both rounds, where programs were deemed suitable, sought to address the criteria – highlighted by meeting the criteria – department has the ability to influence industry to address the needs of government.
- Several Professional services firms applied for these grants but weren't successful.
- Many Applications attempted to address diversity in their applications.
- The Round 1 Assessment Committee had stricter criteria than Round 2, which may have been influenced by the availability of funds in Round 1 being far smaller than in Round 2. This has created a missed opportunity to re-engage and fund Round 1 applications that received similar assessment scores as those recommended for funding in Round 2.

Desktop review. Applicants' ability to meet the Guideline criteria was satisfactory. The assessment Committee categorised applications into four groups:

- Highly suitable and recommended for funding;
- Suitable and recommended for funding;
- Suitable but not recommended for funding; and
- Not suitable.

The applications of suitable quality or higher for each of the rounds were:

- Round 1 had a total of 31 'suitable' to 'highly-suitable' applications (of which 8 were awarded funding).
- Round 2 had a total of 24 'suitable' to 'highly-suitable' applications (of which 18 were awarded funding).

This break-down in assessment and funding outcomes is reflected graphically in Figure 15.

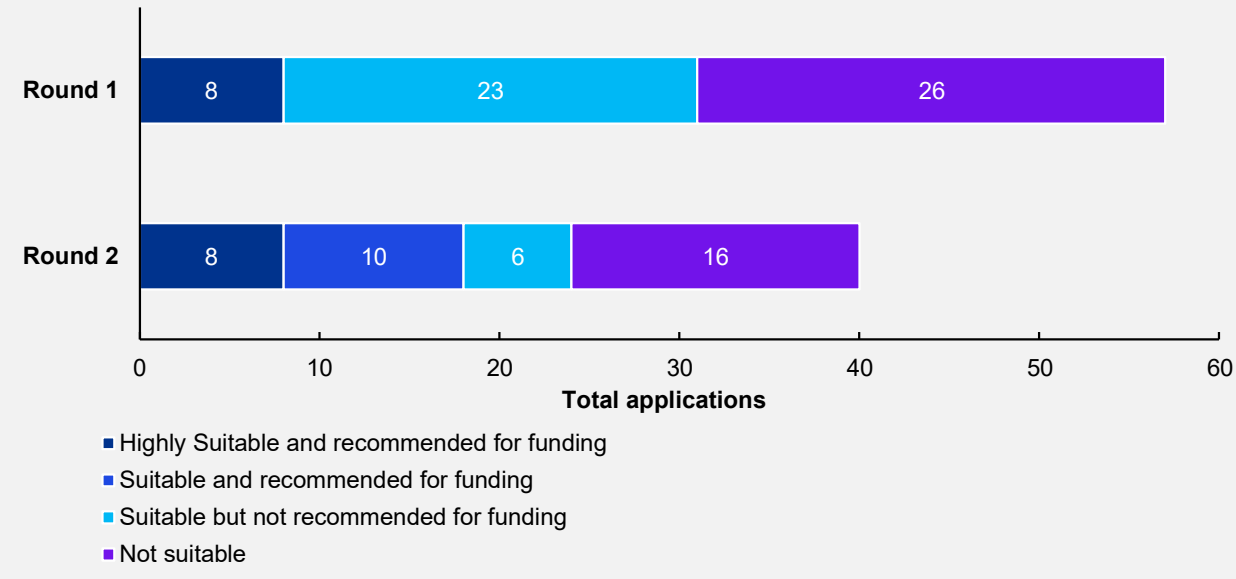


Figure 15: Assessment Committee outcomes for CSSPIF Round 1 and Round 2 (Source: CSSPIF Round 1 and Round 2 grant applications).

11.3.3.1 Applicants have responded well to the Program's emphasis on diversity

Desktop review. The analysis of applications also highlighted that many applicants attempted to address the objective of the CSSPIF to increase the representation of underrepresented cohorts in the cyber security

industry. This increased over time, presumably after the Guidelines were updated to emphasise diversity in Round 2. As mentioned in section 11.1.1, the Round 1 Guidelines aimed to increase the representation of women in the cyber security industry. Whereas the Round 2 Guidelines additionally aimed to increase the representation of Indigenous Australia, regional and remote based workers, and neurodiverse individuals in the cyber security industry. As mentioned above, a large proportion of applicants addressed this aspect of the Guidelines, also emphasising that industry are attentive to the CSSPIF objectives and criteria set out by the Department:

- In Round 1, five out of the eight successful applicants mention a focus on underrepresented cohorts. Of these, four mentioned women, two mentioned the Indigenous and Torres Strait Islander cohort, and one mentioned the rural and remote cohort.
- In Round 2, 14 out of the 18 successful applicants mentioned a focus on underrepresented cohorts. Of these, 13 mentioned women, women mentioned the Indigenous and Torres Strait Islander cohort, six mentioned the neuro-diverse cohort, four mentioned the rural and remote cohort and three mentioned other underrepresented cohorts (e.g. veterans and disability).

This break-down is illustrated in Figure 16.

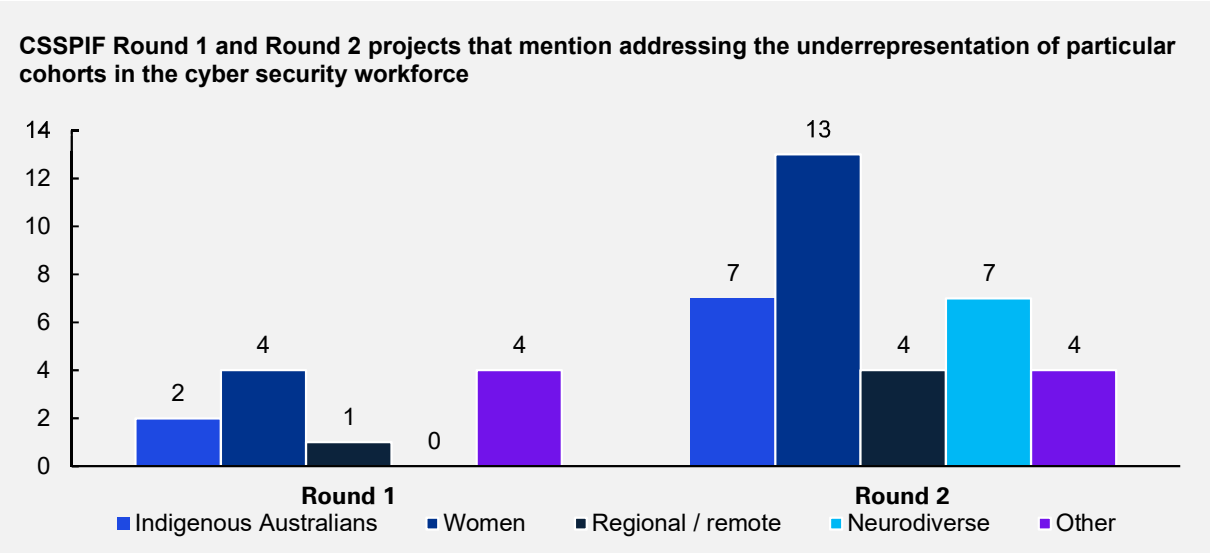


Figure 16: CSSPIF Round 1 and Round 2 projects that mention addressing the underrepresentation of particular cohorts in the cyber security workforce (Source: CSSPIF Round 1 and Round 2 grant applications).

11.3.3.2 Applicants have grown and diversified project partnerships

Desktop review. The analysis of applications also highlighted that many applicants attempted to address the objective of the CSSPIF to improve collaboration between industry and the education sector (see Appendix F):

- Round 1 with 9 government, 15 Industry, 9 education sector and 2 other organisations (including peak and professional bodies and non-government organisations [NGOs]).
- Round 2 with 3 government, 36 Industry, 22 education sector and 13 other organisations (including peak and professional bodies, NGOs and recruitment agencies).

As mentioned in section 11.1.1, the Round 1 Guidelines allowed for government agencies to submit applications. Whereas the Round 2 Guidelines limited the eligibility of lead applicants to non-government organisations. It is evident in Figure 17, that applicants were attentive to the change in the Guideline requirements, with the proportion of government agencies dropping from 26 per cent in Round 1 to 3 per cent in Round 2.

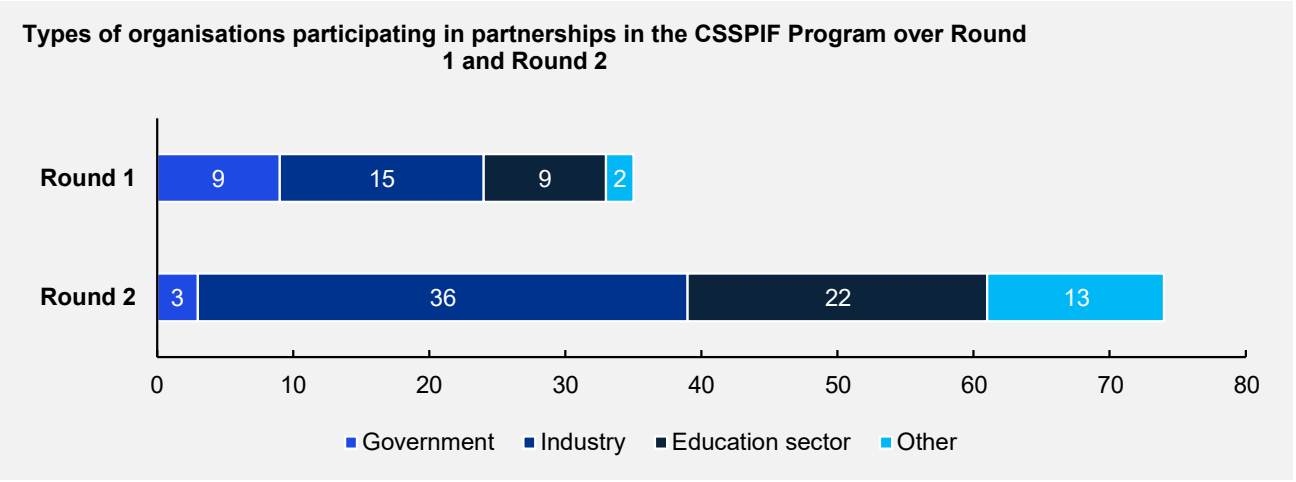


Figure 17: Types of organisations participating in partnerships in the CSSPIF Program over Round 1 and Round 2 (Source: CSSPIF Round 1 and Round 2 grant applications).

11.3.3.3 The Assessment Committee's risk appetite was influenced by the availability of funds

Desktop research. Committee's risk appetite appeared to be influenced by the availability of funds. Desktop research revealed that Round 1 had a higher number of applications (n=57) and less funding ($9.1 million) allocated, and Round 2 had a lower number of applications (n=40) and more funding available ($60.1 million). In Round 1, the Department tried to mitigate the risk of over allocating the funds they had by having stricter criteria thresholds. The minimum assessment score for applications recommended for funding in Round 1 was 82, which is 7 points higher than the minimum for Round 2 (n=75). The average assessment rating value of 'suitable and recommended for funding' applications was significantly higher (i.e. greater than 5 per cent) in Round 1 (n=88.3) than in Round 2 (n=82.4). As a result, Round 2 has recommended funding some projects whose applications received lower assessment rating scores than some projects in Round 1 who were deemed suitable but not recommended for funding. This distribution of assessment score attributes is reflected in Table 10 below.

Table 10. Assessment score attributes of Round 1 and 2 applications.

Attribute	Round 1	Round 2
Average assessment score - funded	88.3	82.4
Maximum score of applications recommended for funding	90	93
Minimum score of applications recommended for funding	82	75
Average assessment score - suitable/highly suitable (whether recommended for funding or not)	78.6	79.8
Count of Round 1 'suitable' Applications that were not recommended for funding but received assessment scores within the same range (75-93) as applications recommended for funding in Round 2.	14	-

As shown in Table 10, 14 applications deemed suitable but not funded in Round 1 received assessment scores within the same range as applications recommended for funding in Round 2 (i.e. 75-93). Of these, half (n=7) re-applied in Round 2, of which 5 were successful and recommended for funding in Round 2; while the other half (n=7) did not re-apply for Round 2. While it is positive that half re-engaged in the Program for Round 2, there remains the missed opportunity to fund previously 'suitable' but not-funded projects from Round 1 – particularly those whose Round 1 assessment scores were comparable to projects funded in Round 2.

Interviews. Stakeholders suggested that this may be a result of the Department's post-round communications approach to unsuccessful applicants.[122] They indicated that the Department should provide a more transparent response to unsuccessful applicants to provide them with appropriate feedback and areas that need to be addressed to be considered for the next round. Departmental stakeholders noted that due to the large number

[122] Consultation C, Consultation N.

of applicants in Round 1 and small proportion of funding, the government committed a larger funding value for Round 2, expecting that the number of applications would be equivalent or larger.[123] As this did not occur, the lowest score for Round 2 applications that were recommended for funding was 75, compared to 85 for Round 1. Some stakeholders queried as to whether the 'Innovation' factor in the Program may have been affected by stringent risk management tools in assessment committee.

11.3.3.4 Over time, a greater number of projects have benefited from larger financial co-contributions from industry

Desktop research. Government funding committed under the CSSPIF Program equates to $33.6M with an additional co-funding of $55.1M by industry and the education sector. Figure 14 further depicts that the Round 2 grant recipients have proposed to commit a larger proportion of funding, equating to 65 per cent, than Round 1 applicants, equating to 51 per cent. Additionally, desktop research found that Round 2 applicants, that were recommended for funding, proposed higher average funded projects, with an average request for $1,411,490 of grant funding. This was compared with an average request for $1,027,602 of grant funding in Round 1. Figure 18 further depicts that successful applicants in Round 2 generally requested a larger amount of grant funding. This may suggest that applicants were more willing to put up significant co-contributions or applicants were better resourced to put forward significant co-contributions. It is unclear if the Committee places a high, medium, or low weight on the scale of co-contribution by applicants when considering applications.

Figure 19: The x in the chart is the mean values, the average ask for grant funding from successful grant recipients increase from $1,027,602 in Round 1 to $1,411,490 in Round 2. Round 1 funding requests ranged from $257,167 to $2,355,923, see whiskers. Round 2 funding requests ranged from $250,000 to $3,000,000, see whiskers.

The box represents quartile 2 and quartile 3 of requested grant funding.

This figure shows that grant recipients requested a higher amount of project funding, meaning their co-contribution was also higher showing an increased investment and interest in growing the cyber security workforce pipeline.

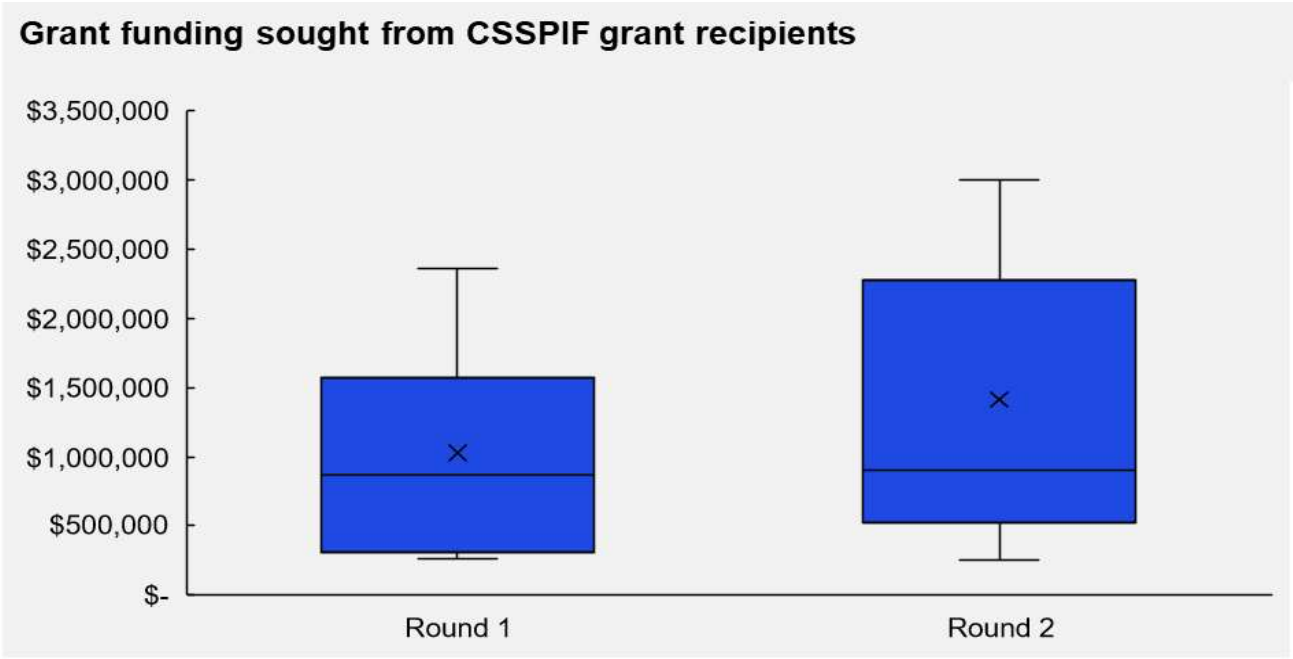


Figure 18: Grant funding sought from CSSPIF grant recipients in Round 1 and Round 2 (Source: CSSPIF Round 1 and Round 2 grant applications).

[123] Consultation C, Consultation P.

11.4 Short-term outputs and outcomes of the CSSPIF Program

This section presents findings related to the short-term outputs and outcomes of the CSSPIF Program. The evaluation found that the CSSPIF Program's overarching aim of increasing networks to support workforce pipeline appears to have been progressed by the CSSPIF Program design and implementation. The CSSPIF Program is achieving this aim through four key areas (detailed below in this section):

1. Increasing cyber security workforce pipeline activations through CSSPIF Program investments;
2. Increasing diversity in the cyber security workforce;
3. Increasing the quality and quantity of cyber security professionals in Australia; and
4. Improving collaboration between industry and the education sector.

11.4.1 CSSPIF projects are encouraging industry co-investment

11.4.1 Key Findings

- The CSSPIF Program has supported the growth of the cyber security workforce pipeline.
- The total investment under the Program from all sources (government, industry and the education sector) is $88.7M over three years.
- The funded projects address activation of skills development across the workforce pipeline, with particular emphasis on post-secondary school cohorts.

Desktop review. To date, 8 contracts signed with a further 18 expected to be executed in FY23-24. Round 2 recipient announcements have been delayed due to the 2022 Federal Election. The significant delay may impact on performance of planned projects, due to major project schedule changes.

The total investment under the Program from all sources is $88.7M over three years. Government funding commitment under the CSSPIF Program equates to $33.6M with an additional co-funding of $55.1M by industry and the education sector (see Figure 14). This demonstrates that the CSSPIF program has successfully driven industry and the education sector to significantly invest in the growth of the cyber security workforce.

11.4.2 CSSPIF projects are more responsive to diversity issues in the cyber security workforce

11.4.2 Key Findings

- The CSSPIF design supports the increase in workforce participation for a number of underrepresented segments of society in the cyber.

Desktop research. Survey responses and stakeholder consultations suggests that the design of the CSSPIF Program is conducive to improving workforce participation for underrepresented population groups in the cyber security industry. Five out of the eight Round 1 projects and 14 out of the 18 Round 2 projects have mentioned in their grant application that they will support increasing the representation of these cohorts. Figure 16 depicts the cohorts that various projects are targeting the cohorts mentioned in the CSSPIF intended outcomes, these cohorts included women, Indigenous Australia, regional and remote based workers, and neuro diverse individuals. Figure 11 reflects survey respondent perspectives on the design of the Program supporting cyber security industry workforce diversity.

It is currently too early to determine if the cyber security workforce participation of underrepresented cohorts who have been in contact with CSSPIF project has actually increased.

11.4.3 CSSPIF projects are supporting industry efforts to increase the quality and quantity of cyber security professionals in Australia

11.4.3 Key Findings

- The CSSPIF design supports the increase in the quality and quantity of cyber security professionals in Australia.

Desktop research. The funded projects are addressing activation of skills development across the workforce pipeline, with particular emphasis on post-secondary school cohorts. This distribution can be expected to support increasing the quality and quantity of cyber security professionals in Australia. Figure 19 depicts the intended beneficiaries of Round 1 and Round 2 CSSPIF projects, refer to Appendix E (section 12.2) for detail on the project names for each CSSPIF Round.

Figure 19: Distribution of projects targeting audiences across the cyber industry talent pipeline (Source: CSSPIF Round 1 and Round 2 grant applications). Number indicates reference identifier number for each project recommended for funding.

Interviews. Grant recipients agreed that the CSSPIF provided an opportunity for them to grow the cyber security workforce. Some grant recipients indicated that they were planning to implement their respective initiatives in the future, however, the CSSPIF grant opportunity allowed them to drive their initiative forward sooner to enable rapid growth of the cyber security workforce to meet Australia's needs.[124]

Survey responses. Most stakeholders who were consulted agree that, while the CSSPIF is making a difference, more needs to be done to support the cyber security workforce pipeline. In addition, most survey respondents most respondents agreed or strongly agreed with the statements that (see Figure 20):

- The CSSPIF is increasing the number/quantity of cyber security professionals in Australia;
- The CSSPIF is improving the quality of cyber security professionals in Australia;
- The CSSPIF has supported industry to build Australia's future pipeline of skilled cyber security professionals;
- The CSSPIF has supported education, training and skills sectors to build Australia's future pipeline of skilled cyber security professionals; and

[124] Consultation J.

- The CSSPIF grant program is needed to grow the workforce and support the sector.

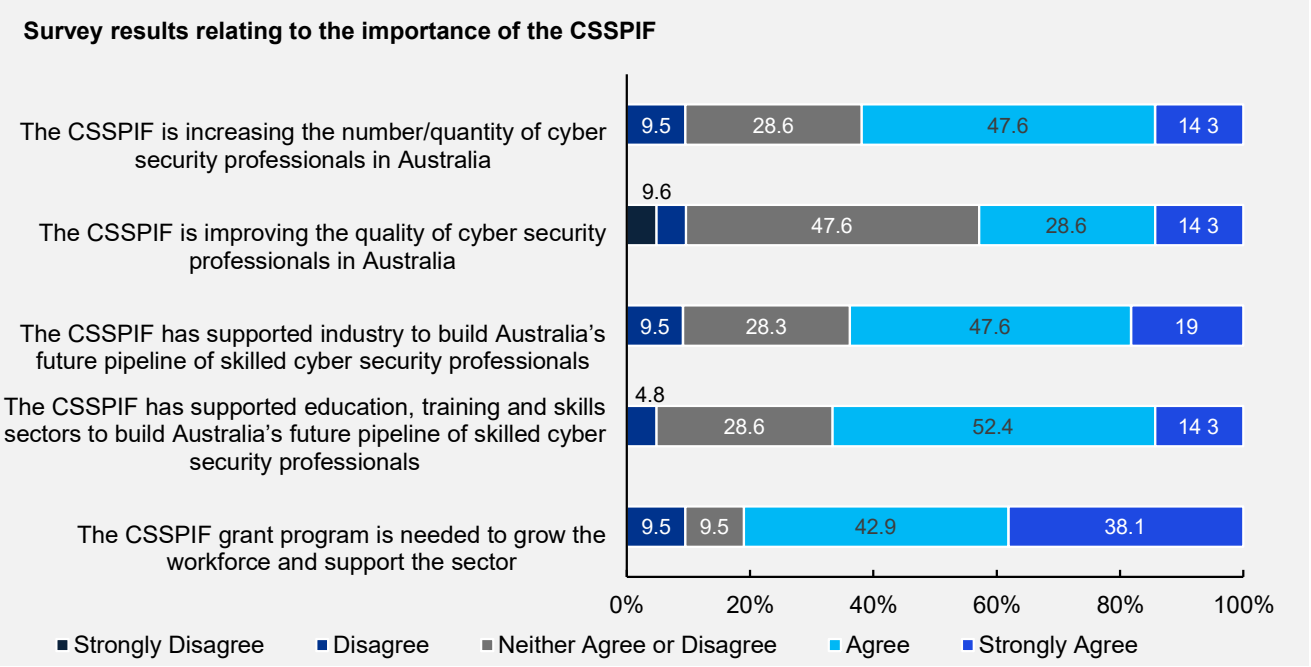


Figure 20: Survey results relating to the importance of the CSSPIF (Source: KPMG CSSPIF Survey, 2022, n=21)

11.4.4 CSSPIF projects are improving collaboration between industry and the education sector

11.4.4 Key Findings

- The CSSPIF design actively promotes partnerships, fostering and catalysing networks and relationships, with a total of 109 organisations participating in partnerships established through Rounds 1 and Round 2.

Desktop research. The design of the CSSPIF achieved the program objective of increasing partnerships to support workforce pipeline. The CSSPIF design actively promotes partnerships, fostering and catalysing networks and relationships. Although some stakeholders indicated that arranging the formal partnerships was a challenge to achieve within the funding round timeframes, and some potential applicants may have been unable to meet this timeframe, Rounds 1 and 2 have nonetheless established formal partnerships between some 109 organisations. Partners include a range of different organisations, spanning government agencies, industry organisations, education sector organisation, peak bodies, non-government organisations and recruitment agencies. Figure 17 depicts the types of organisations that are participating in partnerships. Appendix F maps the partnerships formed in CSSPIF Rounds 1 and 2. Round 1 saw a larger proportion of government agencies participate in the CSSPIF Program round compared to Round 2. Round 2 saw a significant increase in the number and proportion of industry organisations that participated in the CSSPIF Program round.

Interviews. Stakeholders expressed that the CSSPIF Program encouraged organisations to form formal partnerships that would not have occurred otherwise. Stakeholders indicated that the partnerships formed will have positive implications in the future to support the quality and quantity of the cyber security workforce. Moreover, survey respondents agreed (n=21, 76.2 per cent) that the CSSPIF Program is improving collaboration between industry and the education, skills and training sectors.

11.4.5 The funds remaining are significant and are dependent on industry capacity to co-invest at least another $34.7M

11.4.5 Key Findings

- The volume of funds remaining to be allocated in future rounds will be significant, at $34.7 million remaining. Another round of the CSSPIF is dependent on industry's capacity to co-invest a minimum of $34.7 million.

Desktop research. When the successful Round 2 applicants are announced, the volume of funds remaining to be allocated in future rounds will be significant, at $34.7 million remaining (see Figure 21). The implication is that, if future funding rounds are to be run, the Department will need to do in-depth research to understand if the broader digital and cyber security industries and education sector have the capacity to co-invest at least $34.7 million. To date, the industry and education sector have already co-invested $55.1 million in CSSPIF projects (see Figure 14). If this market capacity research is not undertaken, the Department risks not reaching an audience with the financial capacity to participate in the Program under the current guidelines.

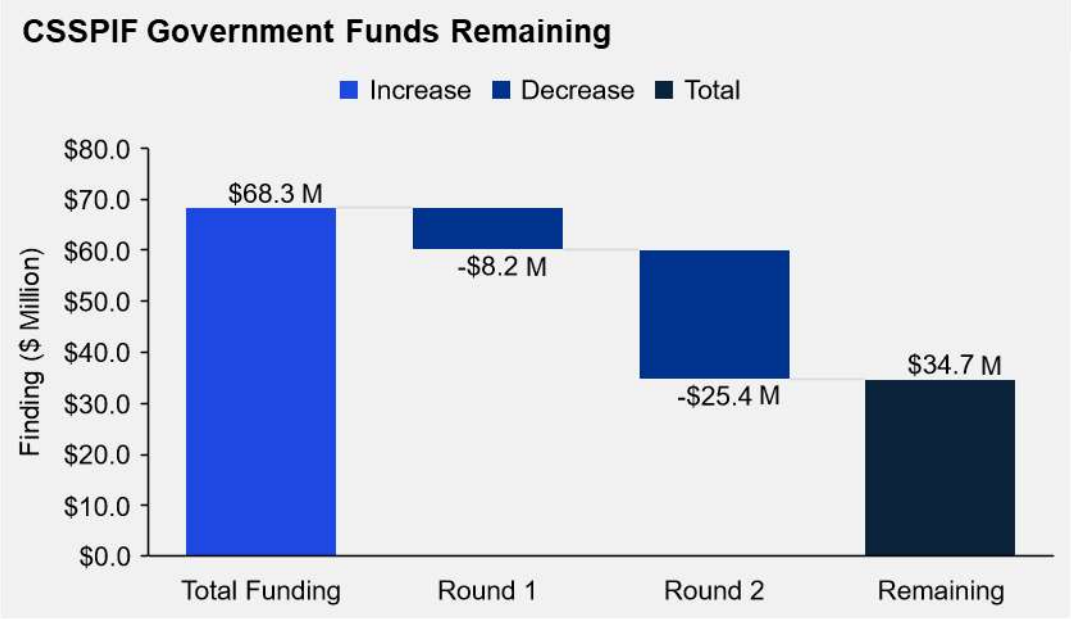


Figure 21: CSSPIF Government Funds Remaining (Source CSSPIF Round 1 and Round 2 grant applications).

Interviews. Stakeholder consultation highlighted the need for the government to continue to drive the growth of the cyber security workforce pipeline. The Department has an opportunity to support this effort with the remaining $34.7 million in funding.

11.4.6 External factors impacting CSSPIF program outputs and outcomes

11.4.6 Key Findings

- COVID-19-related disruptions to the economy do not appear to have deterred industry co-investment in CSSPIF projects, but may have affected the volume of applications received by the Department between Rounds 1 and 2.
- COVID-19-related disruptions to the economy Impacted education and training providers who in some cases faced staff headcount reductions in areas that would be involved in developing grant applications.
- There was limited evidence of coordination between the Department and cyber industry, recruitment and education peak bodies or states and territory governments.
- Government agencies, including ASD, Home Affairs, and the Department of Education and the Department of Employment and Workplace Relations, have associations with the CSSPIF. There was limited evidence of coordination on grant round promotion and communication between these Government agencies.

11.4.6.1 The COVID-19 pandemic has likely affected some potential applicants, but has not materially deterred growth in industry co-investment

Desktop research. Environmental factors appear to have had minimal short-term impact in disrupting program implementation and project co-investment but project roll-out and take up has been affected. As shown in Figure 14 and Figure 18, despite the economic impact of the pandemic, industry co-investment in projects increased between Rounds 1 and 2. However, it is likely that the COVID-19 pandemic affected program engagement as the hardest hit organisations in the cyber industry were smaller-sized firms (representing the greatest proportion of the industry), and the education and training sectors experienced significant structural changes to staffing levels due to lost international student revenues. Notably, the volume of applications received was lower for Round 2 than Round 1. It is unknown how many potential applicants chose not to apply for grants through this Program due to the economic impact of coinciding macroeconomic factors which may have reduced their capacity to prepare applications or meet the financial eligibility requirements (discussed in section 11.1.4.2).

11.4.6.2 The skills shortage for the industry at large is a key risk to CSSPIF Project schedule milestones and outcomes.

Interviews. Stakeholders consulted for this evaluation have found it difficult to recruit suitable cyber security professionals to deliver the training that is core to their CSSPIF project.[125] Projects run from non-metropolitan areas found this to be a greater issue than their metropolitan counterparts. This broader issue around recruitment of cyber security trainers is described further in section 10.1.4.2.

11.4.6.3 The Program is situated in a busy, complicated digital and cyber policy space vying for engagement from industry and key stakeholders

Desktop research. Activities that aim to improve the future cyber security workforce pipeline fall within the remit of multiple government agencies, including DISR, ASD, Home Affairs, and the Department of Education and the Department of Employment and Workplace Relations (see Figure 23). Section 10.3 of this explores the role of Government and that there are several programs of activity at the Federal, State and Territory government level that seek to address the gap in supply of skilled workers for the cyber security sector.

Interviews. While many stakeholders noted that there is a lack of clarity on how the programs fit together to address the larger issue, it was beyond the scope of this evaluation to explore this issue further.

Survey responses. Stakeholder opinion was split as to whether the role and opportunity presented by the CSSPIF, alongside other federal and state government programs, is clear (see Figure 22).

[125] Consultation G, Consultation O.

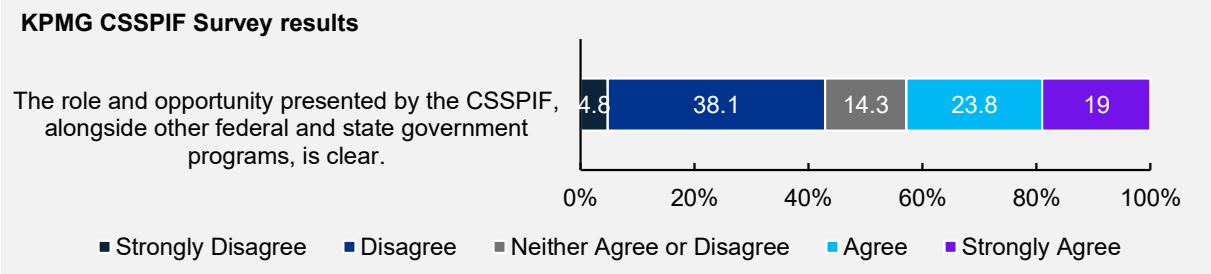


Figure 22: KPMG CSSPIF Survey, question 13: 'The role and opportunity presented by the CSSPIF, alongside other federal and state government programs, is clear'. (Source: KPMG CSSPIF Survey Question 23, 2022, n=21).

Figure 23: Government agencies that are driving initiatives to improve the future cyber security workforce pipeline.

12 Appendix E – Cyber Security Workforce Pipeline

This appendix provides graphics that illustrate the distribution of cyber security workforce growth initiatives across the workforce pipeline.

12.1 Plain Graphic of the cyber security talent pipeline

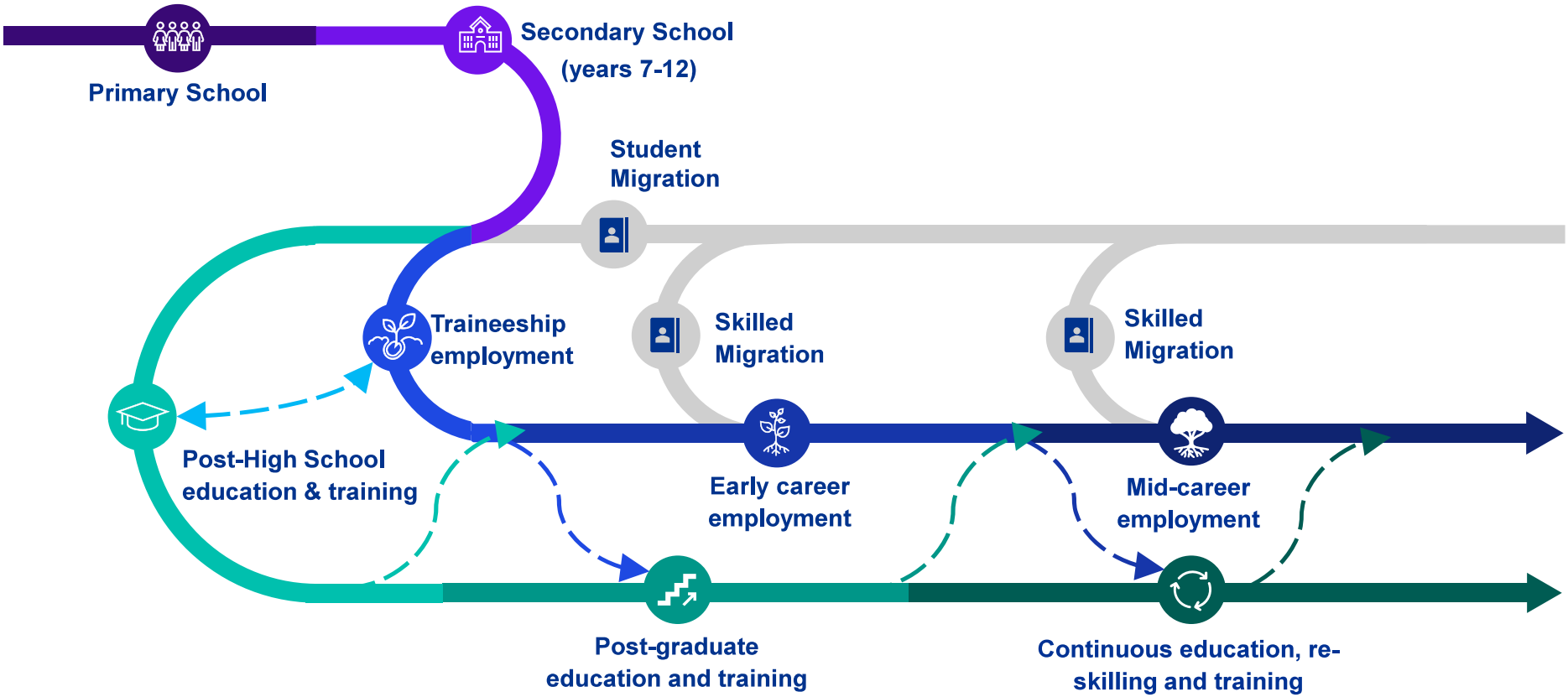


Figure 24. Diagram of the cyber security talent pipeline.

12.2 Talent pipeline mapping of CSSPIF-funded projects

Distribution of projects targeting audiences across the cyber industry talent pipeline

Figure 25. Talent pipeline mapping of CSSPIF-funded projects. Numbers refer the unique identifier for each project recommended for funding.

Table 11: Round 1 projects corresponding to workforce pipeline mapping.

No.	Round 1 Project
1	The partnership for new cybersecurity professionals, skills and employment
2	Regional Western Australia Cybersecurity Skills Expansion Project
3	Gold Coast Cyber Studio
4	Cyber Innovation Training Hub (Tasmania)
5	NSW Workforce and Skills Development Program
6	Innovate to Grow – Cybersecurity (I2G-Cyber)
7	AUSTCYBER AND MICROSOFT CYBER SECURITY TRAINEESHIP PROGRAM (CSTP)
8	Cyber STEPs: secondary to tertiary education partnerships

Table 12: Round 2 projects corresponding to workforce pipeline mapping.

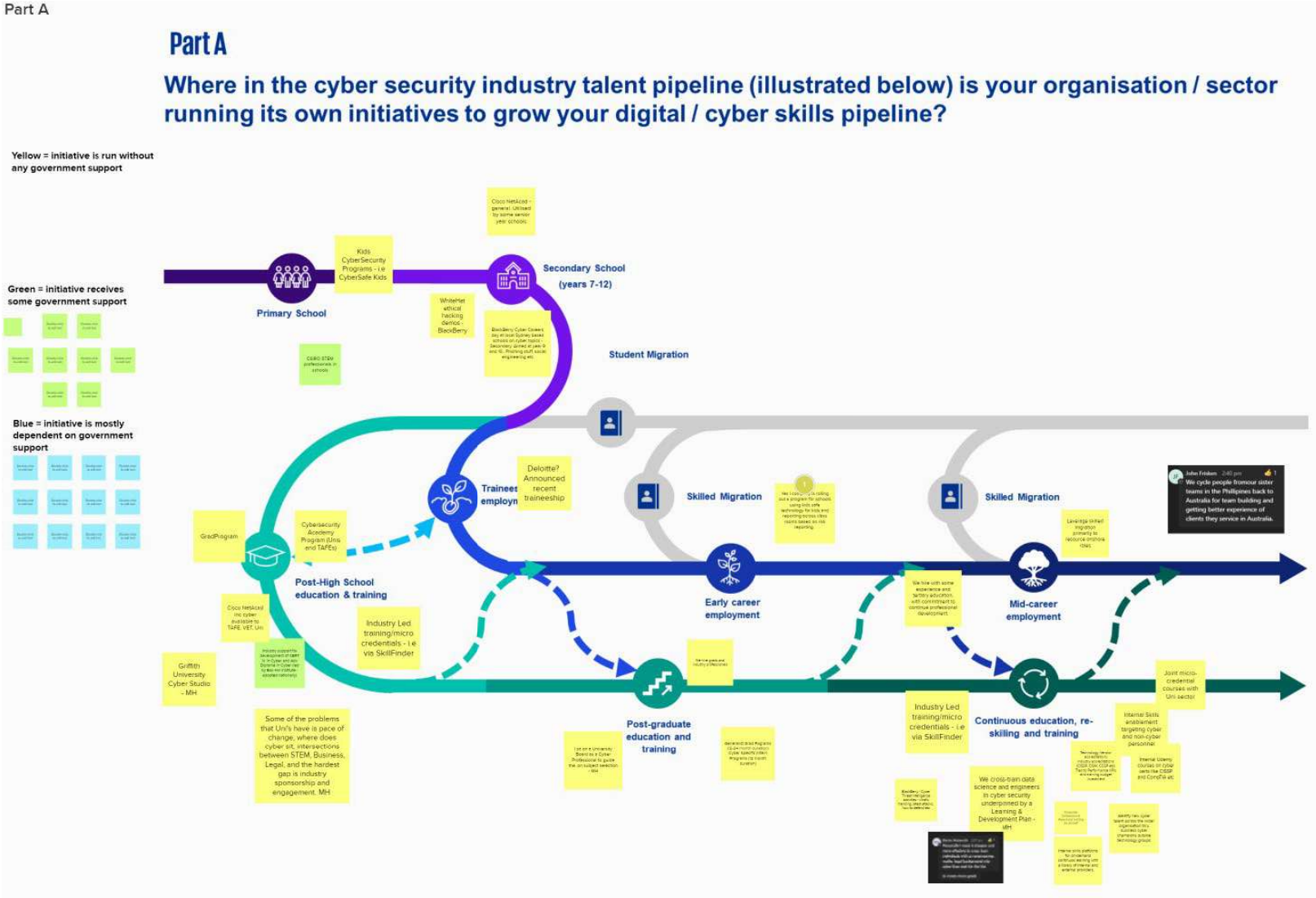
No.	Round 2 Project
1	UniCyber – Nationally Consistent Undergraduate Courseware in Cyber Security
2	Willyama Cyber Traineeship Program (WCTP)
3	Increasing the South East Queensland (SEQ) Cyber Security Workforce
4	CYNAPSE: Benchmarking & Growing Australia's Cyber Operations Workforce
5	Growing the cyber security workforce through UTS Cyber Security Institute
6	Multi-Pathway Talent Development for a Diversified Cyber Security Workforce
7	Inclusive Cyber Skills Strengths Based Training & Employment Program

No.	Round 2 Project
8	Threat Hunting and Incident Response Training Platform
9	Transforming Water Industry IoT and OT cybersecurity skills
10	The Centre for Cyber Training
11	Indigenous ICT Cyber Employment Pathway
12	Develop a Cross-disciplinary Cyber Security Workforce Training Program
13	Cyber Security Microcredential and Employment-Ready Program
14	Cyber skills for Boards, Teachers and Security Professionals
15	Australia's first cyber and digital forensics tactical training facility
16	Cyber Territory Skills Hub
17	WorkVentures Transition to Cybersecurity Career Accelerator
18	Purple Team Australia Program (PTAP)

12.3 Other industry activities (mural board)

High-resolution copies of this whiteboard from the Cyber Security Workforce Growth Programs Workshop are provided in Attachment D of this report.

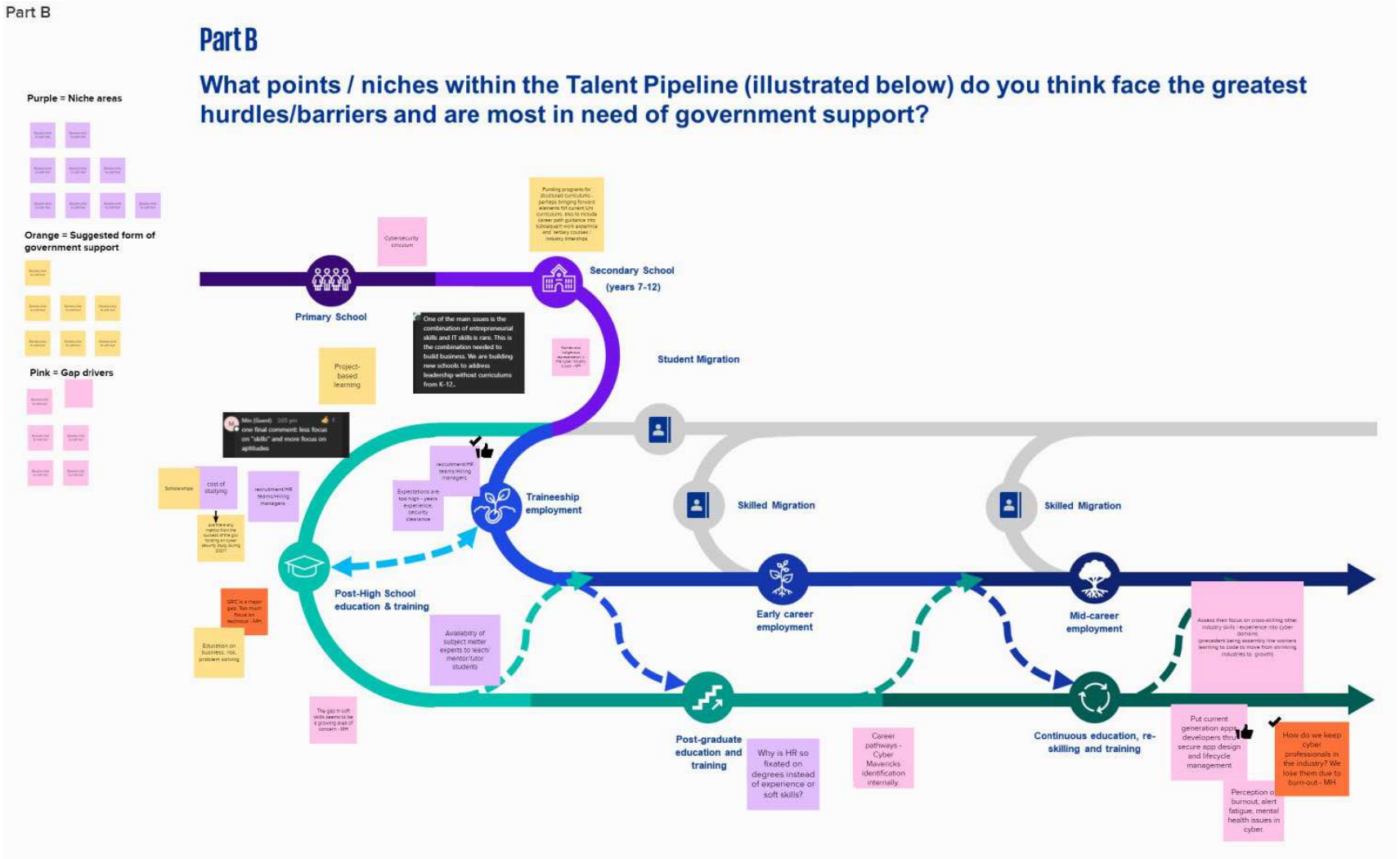
Figure 26. Industry-led initiatives addressing the cyber security industry talent pipeline, as identified by the AIIA Cyber Security PAN.



12.4 Other government support opportunities (mural board)

High-resolution copies of this whiteboard from the Cyber Security Workforce Growth Programs Workshop are provided in Attachment D of this report.

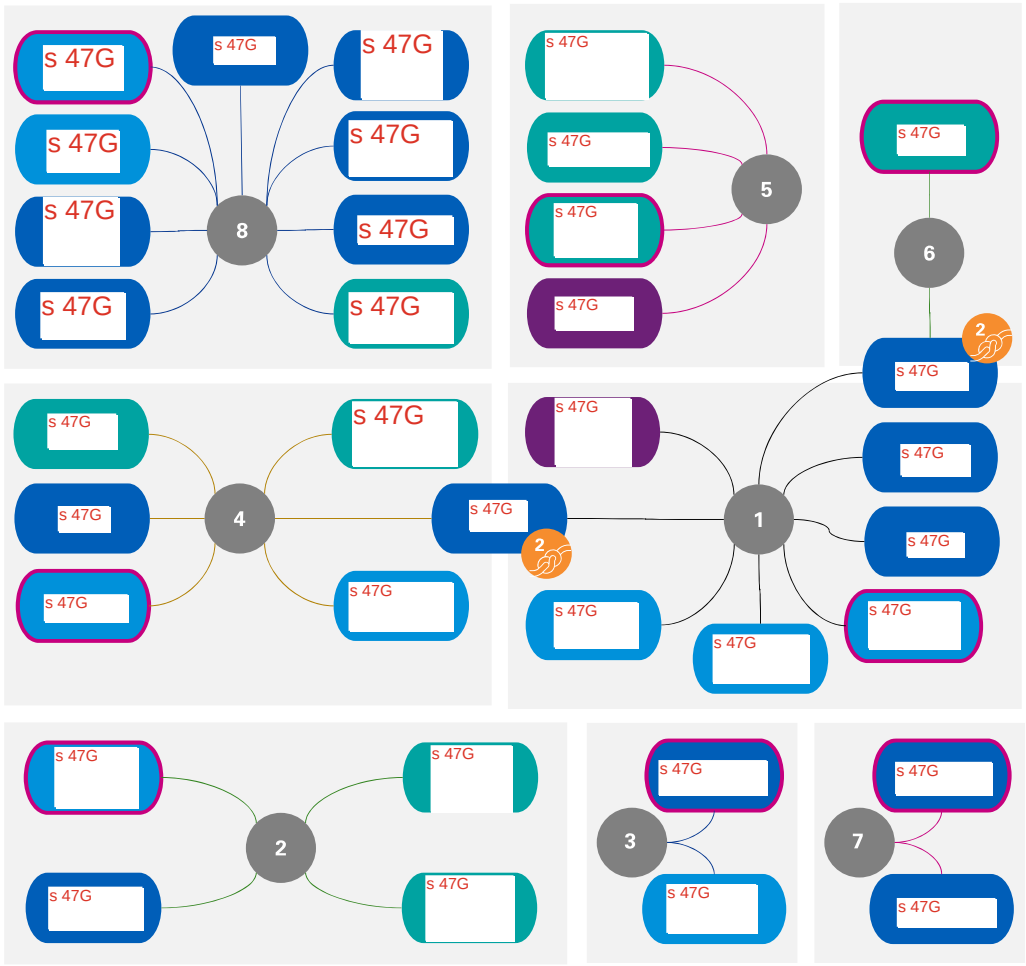
Figure 27. Other niches in the cyber security industry talent pipeline facing barriers in need of government support, as identified by the AIIA Cyber Security PAN.



13 Appendix F – CSSPIF partnerships and networks

This appendix provides graphics that illustrate the connections between the partnerships and networks fostered through CSSPIF-funded projects.

Round 1 – Partnership Mapping

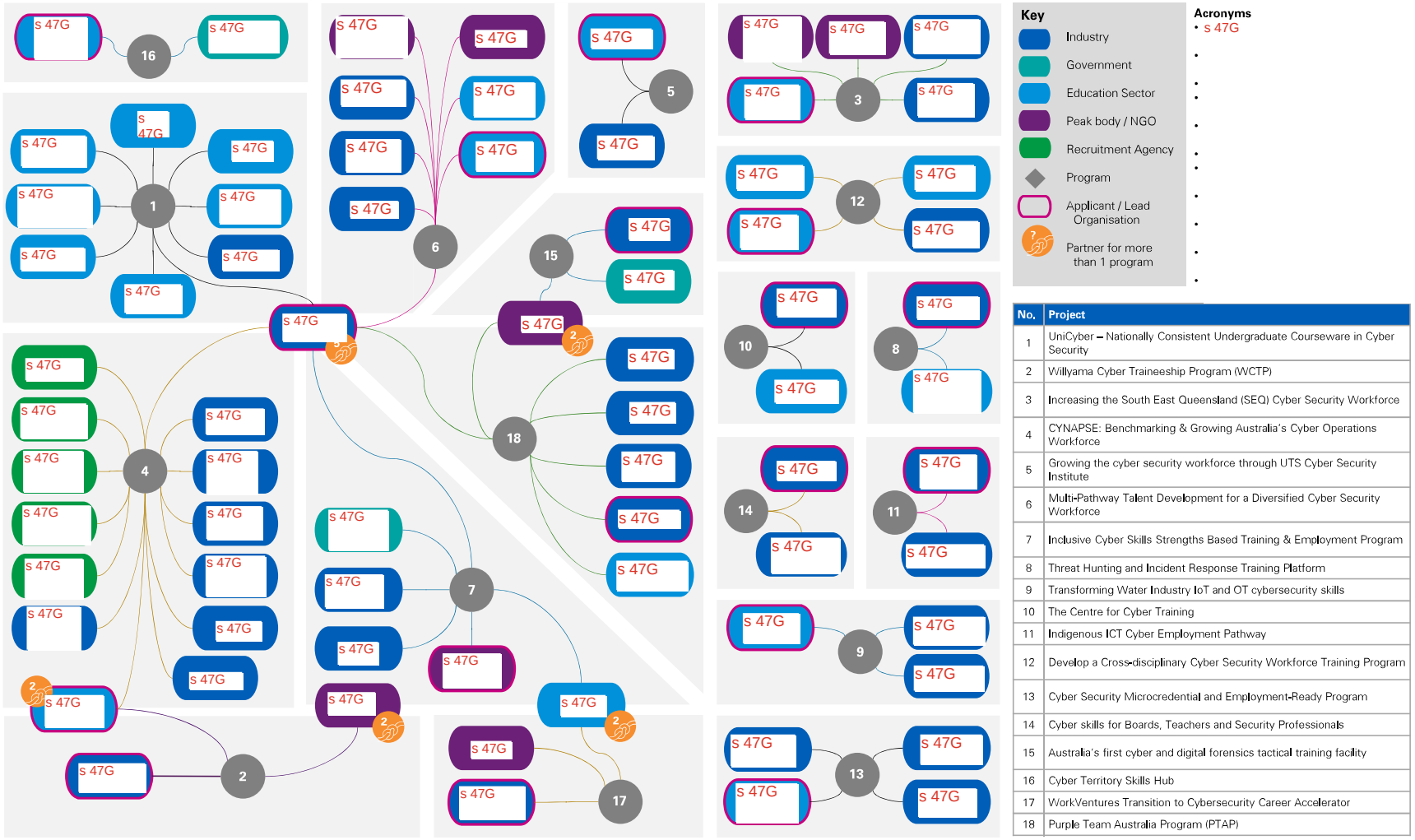


No.	Project
1	The partnership for new cybersecurity professionals, skills and employment
2	Regional Western Australia Cybersecurity Skills Expansion Project
3	Gold Coast Cyber Studio
4	Cyber Innovation Training Hub (Tasmania)
5	NSW Workforce and Skills Development Program
6	Innovate to Grow – Cybersecurity (I2G-Cyber)
7	AUSTCYBER AND MICROSOFT CYBER SECURITY TRAINEESHIP PROGRAM (CSTP)
8	Cyber STEPs: secondary to tertiary education partnerships

s 47G

Figure 28: CSSPIF Round 1 Partnership Map.

Round 2 – Partnership mapping



No.	Project
1	UniCyber – Nationally Consistent Undergraduate Courseware in Cyber Security
2	Willyama Cyber Traineeship Program (WCTP)
3	Increasing the South East Queensland (SEQ) Cyber Security Workforce
4	CYNAPSE: Benchmarking & Growing Australia's Cyber Operations Workforce
5	Growing the cyber security workforce through UTS Cyber Security Institute
6	Multi-Pathway Talent Development for a Diversified Cyber Security Workforce
7	Inclusive Cyber Skills Strengths Based Training & Employment Program
8	Threat Hunting and Incident Response Training Platform
9	Transforming Water Industry IoT and OT cybersecurity skills
10	The Centre for Cyber Training
11	Indigenous ICT Cyber Employment Pathway
12	Develop a Cross-disciplinary Cyber Security Workforce Training Program
13	Cyber Security Microcredential and Employment-Ready Program
14	Cyber skills for Boards, Teachers and Security Professionals
15	Australia's first cyber and digital forensics tactical training facility
16	Cyber Territory Skills Hub
17	WorkVentures Transition to Cybersecurity Career Accelerator
18	Purple Team Australia Program (PTAP)

Figure 29: CSSPIF Round 2 Partnership Map.

Contact us

S 22 , **Partner**
ra
S 22 @kpmg.com.au

S 22 , **Partner**
KPMG Canberra
S 22 @kpmg.com.au

S 22 , **Director**
KPMG Canberra
S 22 @kpmg.com.au

S 22 , **Associate Director**
Canberra
S 22 @kpmg.com.au

com.au