



Australian Government
Department of Home Affairs

Submission

For decision

PDMS Ref. Number: MS24-000335

Date of Clearance: 21/03/2024

To Minister for Home Affairs
Minister for Cyber Security

Subject Amendments to Financial Framework (Supplementary Powers)
Regulations 1997 - Cyber Security Strategy Grant Programs

Timing For consideration by 28 March 2024, as agreed by George Threadgold, to meet the requirements for the Executive Council meeting scheduled for 9 May 2024.

Recommendations

That you:

1. agree to the proposed amendments to *Schedule 1AB of the Financial Framework (Supplementary Powers) Regulations 1997* to establish legislative authority for three grant programs under the 2023-2030 Australian Cyber Security Strategy; and (agreed) / not agreed
2. sign the attached letter to the Minister for Finance, the Senator the Hon. Katy Gallagher, seeking agreement to insert the items into *Schedule 1AB of the Financial Framework (Supplementary Powers) Regulations 1997*. (signed) / please discuss

Minister's Comments

Noting clear advice that this is an ordinary and commonly used process to deliver grants programs such as these.

Minister for Home Affairs
Minister for Cyber Security

Date: 5/4/2024

Signature.....

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Key Issues

1. This submission seeks your agreement to proposed amendments to Schedule 1AB of the *Financial Framework (Supplementary Powers) Regulations 1997* (FF(SP) Regulations) to ensure robust legislative authority for Government spending on three separate grant programs funded as part of the *2023-2030 Australian Cyber Security Strategy* (the Strategy).
2. The three grant programs to be impacted by the proposed amendments are:

s. 22(1)(a)(ii)

- o \$1.9 million - Professionalisation of the Cyber Workforce Grant Program (two year program from 2023-24).
3. These grant programs are significant deliverables under the Strategy and will achieve outcomes related to strengthening small businesses and citizens, developing world-class threat sharing and building sovereign capability. Timely delivery of these programs in 2024 is crucial for meeting the implementation goals for *Horizon 1* of the Strategy.

Proposed Regulation Amendments

4. Commonwealth expenditure, including one-off or multi-year grant programs, requires constitutional support and express legislative authority prior to undertaking any contracting or spending. New policy proposals that involve Commonwealth expenditure are required to undergo a constitutional and legislative authority risk assessment (CLRA) by the Australian Government Solicitor (AGS).

s. 42(1)

s. 42(1)

s. 42(1)

s. 47E(d)

s. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

s. 47E(d)

Background

10. s. 47C(1)
s. 34(2) s. 47C(1)
s. 47C(1) provided funding for the following grant programs:

s. 22(1)(a)(ii)

- c. The *Professionalisation of the Cyber Workforce* Grant Program will be delivered under Shield 5 of the Strategy. The program will support the cyber security workforce through building a national professionalisation scheme that will provide employers and businesses with the assurance that the workforce is appropriately skilled, while workers know their qualifications and experience are recognised, fit for purpose and support a thriving ecosystem. The program will commence in September 2025 and be delivered over a two year period.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Consultation – internal/external

11. Internal

- Chief Finance Officer
- General Counsel
- Financial Frameworks section
- Refugee and International Law Section

12. External

- Department of Finance
- Australian Government Solicitor

Consultation – Secretary

13. The Secretary was not consulted on this submission.

Client service implications

14. Nil.

Risks and Sensitivities

15. These grant programs are key deliverables under Horizon 1 of the Strategy. Failure to open them this financial year will risk implementation timeframes not being met.

s. 47(1)(b)

Financial/systems/legal/deregulation/media implications

17. Funding for these grant programs was provided as part of the 2023-24 MYEFO process.

18. A dedicated communications plan will be developed for the launch of the grant programs.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Attachments

Attachment A Legislative amendments

s. 42(1)

Attachment C Letter to Minister for Finance

s. 22(1)(a)(ii)

Attachment F Attachment C to Letter

Authorising Officer
Cleared by:
Peter Anstee First Assistant Secretary Cyber and Technology Security Policy Division
Date: 21 March 2024
Mob: s. 22(1)(a)(ii)

Contact Officer: Chris Gower, Assistant Secretary, Cyber Policy and Programs, Ph s. 22(1)(a)(ii)

Through Chief Finance Officer

CC Deputy Secretary Cyber and Infrastructure Security
Assistant Secretary Legislation

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*



OFFICIAL: Sensitive

Legal privilege

MS24-000335

Attachment A

Proposed amendments to Schedule 1AB of the *Financial Framework (Supplementary Powers) Regulations 1997* to include the following grant programs from the *2023-2030 Australian Cyber Security Strategy*.

Item	Program	Objective(s)
s. 22(1)(a)(ii)		
s. 47(1)(b)		

Legal privilege

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Legal privilege

S. 47(1)(b)

Legal privilege
OFFICIAL: Sensitive

s. 42(1)

s. 42(1)

s. 42(1)

s. 42(1)

s. 42(1)

s. 42(1)

s. 42(1)



The Hon Clare O'Neil MP
Minister for Home Affairs
Minister for Cyber Security

Ref No: MS24-000335

Senator the Hon Katy Gallagher
Parliament House
CANBERRA ACT 2600

Dear Minister

Request for a new or amended Schedule 1AB item

I am writing to seek your agreement to insert three new items in Schedule 1AB to the *Financial Framework (Supplementary Powers) Regulations 1997* (the FF(SP) Regulations) to establish legislative authority for government spending on three grant programs:

s. 22(1)(a)(ii)

- the Professionalisation of the Cyber Workforce Grant Program.

This Schedule 1AB amendment is proposed for consideration by the Governor-General at the Federal Executive Council meeting scheduled for 9 May 2024.

Summary of the proposed Commonwealth expenditure

These grant programs will be delivered under the 2023-2030 Australian Cyber Security Strategy (the Strategy). The Strategy supports Program 1.3 Cyber Security within Outcome 1 of the Department of Home Affairs' Portfolio Budget Statement – Protect Australia from national security and criminal threats, and support national resilience, through effective national coordination, policy and strategy development and regional cooperation.

The Strategy sets out the Australian Government's vision to be a world leader in cyber security by 2030. The Strategy has been developed with Australian citizens and businesses at its core and will take a whole-of-nation approach to building cyber resilience. The Strategy is built around six cyber shields:

1. Strong businesses and citizens
2. Safe technology
3. World-class threat sharing and blocking

4. Protected critical infrastructure
5. Sovereign capabilities
6. Resilient region and global leadership

s. 22(1)(a)(ii)

Professionalisation of the Cyber Workforce Grant Program

This program will be delivered under Shield 5 of the Strategy, which outlines Australia's vision of a flourishing cyber industry, enabled by a diverse and professional workforce. The policy objective of this program is to support the cyber security workforce through building a national professionalisation scheme that will provide employers and businesses with the assurance that the workforce is appropriately skilled, while workers know their qualifications and experience are recognised, fit for purpose and support a thriving ecosystem. This program will be implemented through a grant and is expected to commence September 2024 and will be delivered over a two-year period.

Policy authority

Cabinet

Policy authority for two of the programs, s. 22(1)(a)(ii) and the Professionalisation of the Cyber Workforce Grant Program was provided by the 2023-24 Mid-Year Economic and Fiscal Outlook context s. 34(2) s. 22(1)(a)(ii)

s. 22(1)(a)(ii)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Funding information

s. 22(1)(a)(ii)

Professionalisation of the Cyber Workforce Grant Program

Funding of \$8.5 million over three years from 2023-24 to further grow and professionalise the cyber security industry and support start-ups and small and medium enterprises to innovate and commercialise solutions to cyber security challenges, including \$1.9 million over two years from 2023-24 for the Professionalisation of the Cyber Workforce Grant Program, was included in the 2023-24 Mid-Year Economic and Fiscal Outlook under the measure *2023-30 Australian Cyber Security Strategy*. Details are set out in the Mid-Year Economic and Fiscal Outlook 2023-24 Appendix A: Policy decisions since the 2023-24 Budget at page 269. This measure is reflected in the corresponding 2023-24 Portfolio Additional Estimates Statement, under Outcome 1, Program 1.3, Administered expenses at page 31. This grant will be delivered through an open competitive grant program administered by the Business Grants Hub in the Department of Industry, Science and Resources.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Summary of constitutional and legislative authority risks

s. 22(1)(a)(ii)

Professionalisation of the Cyber Workforce Grant Program

s. 42(1)

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

S. 42(1)

To assist your department with drafting the proposed Schedule 1AB amendment and preparing explanatory materials, I have enclosed additional information about the program at s. 22(1)(a)(ii) and **Attachment C**.

Yours sincerely



CLARE O'NEIL

5/4/2024

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

Attachment C

Attachment C: Professionalisation of the Cyber Workforce Grant Program additional information

Description of the proposed new Commonwealth expenditure

The 2023-24 Mid-Year Economic Fiscal Outlook measure *2023-2030 Australian Cyber Security Strategy* (the Strategy), the Government provided grant funding that will support the uplift of Australia's cyber security posture including:

- \$1.9 million - Professionalisation of the Cyber Workforce Grant Program (two year program from 2023-24).

The Strategy was announced by the Hon Clare O'Neil MP, the Minister for Home Affairs and Cyber Security, on 22 November 2023. Details of the announcement are available at [Cyber strategy signals generational shift in response to growing threat \(homeaffairs.gov.au\)](https://www.homeaffairs.gov.au/cyber-strategy-signals-generational-shift-in-response-to-growing-threat)

The objective of the Strategy is to improve our cyber security, manage cyber risks and better support individuals and Australian businesses to manage the cyber environment. This is part of the Government's overall objective to ensure that Australia is a world leader in cyber security by 2030.

The Strategy has been developed with Australian citizens and businesses at its core and will take a whole-of-nation approach to building cyber resilience. The Strategy is built around six cyber shields:

1. Strong businesses and citizens
2. Safe technology
3. World-class threat sharing and blocking
4. Protected critical infrastructure
5. Sovereign capabilities
6. Resilient region and global leadership

The Professionalisation of the Cyber Workforce Grant Program will be delivered as an initiative under Shield 5: Sovereign capabilities to professionalise the domestic cyber workforce.

The Professionalisation of the Cyber Workforce Grant Program contributes to the Department of Home Affairs Outcome 1 - Protect Australia from national security and criminal threats, and support national resilience, through effective national coordination, policy and strategy development, and regional cooperation.

The cyber security industry contributes an estimated \$2.4 billion to the economy with significant scope to grow. This industry must be underpinned by a strong cyber workforce to ensure the industry continues to contribute to economic growth and build trust in the digital economy. The industry is lacking clarity in skills qualification and recognition which is a significant barrier for prospective cyber professionals looking to enter the market.

Under the Professionalisation of the Cyber Workforce Grant Program, the Government has allocated a nominal value for the expected funding of the grant. There is one grant available under this program and the value has been determined based on estimated costs required to engage with the industry and build on existing work undertaken to develop a professionalisation scheme in the industry. Due to lack of a national framework, a number of jurisdictions and industry leaders have undertaken work in this area, this project would draw on and build on that work.

The funding will be provided over two years to develop and test a cyber security professionalisation scheme in consultation with key stakeholders including cyber security firms, education providers, skills authorities and certifiers. The design of the pilot and scheme would be required to meet core government expectations to examine the ways tertiary qualifications are better aligned with skills needs now and into the future.

s. 47(1)(b)

Various requirements apply to the funding, including that:

- grant money can only be used to:
 - lead a consortium to develop a professionalisation scheme to ensure clear frameworks for cyber security skills through:
 - a pilot Cyber Security Professionalisation Scheme developed in collaboration with industry;
 - a plan to scale the scheme after the pilot that provides:
 - an increase in industry uptake and participation in the scheme;
 - career pathways for workers in, and seeking to enter, the cyber security workforce;
 - clear guidance for employers and employees regarding skills expectations for accredited professionals; and
 - how the scheme would be self-sustaining and independent from government funding; and

Released by Department of Home Affairs
under the Freedom of Information Act 1982

- engage with stakeholders and undertake research to support building the framework, including existing work and skill recognition schemes within the industry. This will include engaging with appropriate industry and accreditation bodies. States and territories and the Future Skills Organisation;
- the projects need to be additional to an eligible funding recipient's existing work plan;
- activity on eligible projects must be undertaken between 1 July 2024 and 30 June 2026; and
- reporting be provided, including on amounts spent, details of progress on projects and jobs supported by the funding, on a quarterly, annual and (where required) ad hoc basis.

The Professionalisation of the Cyber Workforce Grant Program will be an open competitive grant opportunity. To be eligible, applicants must:

- have an Australian Business Number (ABN);
- be registered for the Goods and Services Tax (GST);
- be located in Australia; and
- have an account with an Australian financial institution,

as well as be one of the following entity types:

- an entity, incorporated in Australia; or
- a not-for-profit organisation.

Joint applications are acceptable, provided you have a lead organisation who is the main driver of the project and is eligible to apply.

Applicants are not eligible to apply if they are:

- an organisation, or their project partner is an organisation, included on the National Redress Scheme's website on the list of 'Institutions that have not joined or signified their intent to join the Scheme';
- an employer of 100 or more employees that has not complied with the Workplace Gender Equality Act (2012);
- an individual;
- a partnership;
- a Regional Development Australia committee;
- an unincorporated association;
- any organisation not included in the list of eligible entities;
- a trust (however, an incorporated trustee may apply on behalf of a trust);

- a Commonwealth, state, territory or local government body (including government business enterprises); or
- a non-corporate Commonwealth entity.

s. 47(1)(b)

s. 42(1)

s. 42(1)

s. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Decisions about Commonwealth expenditure

The grant will be administered in accordance with the Commonwealth resource management framework, including the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) and the *Commonwealth Grants Rules and Guidelines 2017*. Grant opportunity guidelines will be developed by the Department of Home Affairs and information about the grant will be made available on the GrantConnect website (www.grants.gov.au). The grant will be administered by the Business Grants Hub, which is part of the Department of Industry, Science and Resources.

A delegate of the Secretary of the Department of Home Affairs under section 32 of the FFSP Act will be responsible for final spending decisions on Commonwealth funding provided to grant recipients. Final spending decisions will be made by the Assistant Secretary, Cyber Policy and Programs. In addition, the Assistant Secretary is authorised to approve commitment of relevant money for goods and/or services under the PGPA Act.

Availability of independent merits review

Independent merits review is not considered suitable for decisions made in connection with the payments. Funding decisions made at the discretion of the Department's delegate can be excluded from independent merits review due to the allocation of finite resource for each financial year from which all potential claims for a share of the resource cannot be met.

Consultation

The Government consulted extensively with stakeholders and industry during the development of the Strategy. A Strategy discussion paper was released on 27 February 2023, with submissions open up to 15 April 2023. The Department received over 330 written submissions. Public submissions were published on the Department website on 12 September 2023. Stakeholder consultation broadly acknowledged that a prosperous cyber security ecosystem must be built on the foundations provided by a strong domestic cyber security labour market. Feedback supported the idea that the standardisation of cyber professionalization will create a digitally-skilled workforce that companies are confident in employing.

Input to the statement of compatibility with human rights

This amendment is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the Human Rights (Parliamentary Scrutiny) Act 2011.

Human rights implications

This amendment does not engage any of the applicable rights or freedoms.

Conclusion

This proposed amendment is compatible with human rights as it does not raise any human rights issues.



Australian Government
Department of Home Affairs

Submission

For decision

PDMS Ref. Number: MS24-001013

Date of Clearance: 04/11/2024

To Minister for Home Affairs, Minister for Immigration and Multicultural Affairs, Minister for Cyber Security

Subject Grant Opportunity Guidelines - Growing and Professionalising the Cyber Security Industry Program

Timing For consideration by 15 November 2024 (10 business days) in order to ensure timely release of the Grant Opportunity.

Recommendations

That you:

1. approve the release of the Grant Opportunity Guidelines for the Growing and Professionalising the Cyber Security Industry Program (Attachment A); (C) approved / not approved
2. note the Department of Finance and the Department of the Prime Minister and Cabinet agreed the s. 42(1) (C) noted / please discuss

s. 42(1)
3. note the decision maker for this Grant opportunity is a departmental delegate; and (C) noted / please discuss
4. sign the attached letter to the Minister for Finance, Senator the Hon Katy Gallagher, seeking agreement to publicly release the guidelines (Attachment D). (C) signed / not signed

Minister for Home Affairs, Minister for Immigration and Multicultural Affairs, Minister for Cyber Security

Signature.....

Date: 11/11/2024

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Minister's Comments

Key Issues

1. This submission seeks your approval to release the *Growing and Professionalising the Cyber Security Industry Program* Grant Guidelines (the Guidelines) (**Attachment A**), and that you note the related Self-Assessment Risk Analysis (**Attachment B**).
2. As part of the *2023-2030 Australian Cyber Security Strategy* (the Strategy), the Department of Home Affairs (the Department) received funding of \$1.9m s. 34(2) [REDACTED] to release an open grant for the design, promotion and piloting of a professionalisation scheme for Australia's cyber security workforce.

s. 47E(d)

s. 47E(d)

s. 42(1)

s. 42(1)

s. 47E(d)

s. 47E(d)

s. 47E(d)

s. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

6. The Guidelines and Self-Assessment Risk Analysis have been designed in consultation with the Business Grants Hub, PM&C and the Department of Finance according to the *Commonwealth Grants Rules and Guidelines 2017*.

s. 47E(d)

8. The Deputy Secretary, Cyber and Infrastructure Security, Department of Home Affairs will act as the departmental delegate for the grant opportunity.

Background

9. In response to industry calls for greater clarity around how cyber security qualifications and skills map to industry requirements, this grant program will provide \$1.9 million in funding to design, promote and pilot a professionalisation scheme for Australia's cyber security workforce. Funding will be provided over 2 years from 2024-25 to 2025-26.
10. The objectives of the grant program are to:
- establish a pilot industry-led cyber security professionalisation scheme;
 - provide clear career, skills and education pathways for cyber security professionals, and quality assurance for employers about professional qualifications and cyber security experience of job seekers;
 - reduce barriers to entry into the cyber industry;
 - enhance domestic cyber capabilities through professionalising the cyber security workforce; and
 - increase industry and business confidence in Australia's cyber security workforce.
11. The grantee will not be required to develop and implement an accreditation program. However, the successful grantee should ensure the professionalisation scheme is interoperable with existing accreditation frameworks.

Consultation – internal/external

12. Internal – Consultation occurred with the National Office of Cyber Security, Chief Finance Officer, Legal Group and the Financial Frameworks Section.
13. External – The Department has consulted the Department of Finance, Department of Prime Minister and Cabinet, Australian Government Solicitor, Business Grants Hub, Department of Industry Science and Resources, Australian Signals Directorate, Department of Education and the Department of Employment and Workplace Relations.

Consultation – Secretary / Associate Secretary Immigration / ABF Commissioner

14. The Secretary was not consulted on this submission.

Client service implications

15. Not applicable.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Risks and Sensitivities

s. 42(1)

s. 42(1)

s. 47E(d)

s. 47E(d)

s. 47E(d)

s. 47E(d) s. 47C(1)

s. 34(2)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

s. 47E(d)

Financial/systems/legal/deregulation/media implications

22. Funding for these grant programs was provided through the 2023-24 MYEFO process.

Attachments

Attachment A Growing and Professionalising the Cyber Security Industry Grant Opportunity Guidelines

s. 47(1)(b), s. 47E(d)

s. 42(1)

Attachment D Minister Burke to Minister Gallagher - Professionalisation Guidelines

Authorising Officer
Cleared by:
 Hamish Hansford Deputy Secretary Cyber and Infrastructure Security
Date: 04/11/2024 Mob: s. 22(1)(a)(ii)

Contact Officer: Ashley Bell Assistant Secretary, Cyber Policy and Programs, Ph: s. 22(1)(a)(ii) / Mob: s. 22(1)(a)(ii)

CC Office of the Secretary
DS Chief Operating Officer
Group Manager Legal
Chief Finance Officer
First Assistant Secretary Cyber and Technology Security Policy
Assistant Secretary Legislation

Released by Department of Home Affairs
under the Freedom of Information Act 1982



Australian Government

Department of Industry, Science and Resources

Department of Home Affairs

Grant Opportunity Guidelines

Growing and Professionalising the Cyber Security Industry Program

Opening date:	xxxx 2024
Closing date and time:	17:00 Australian Eastern Daylight Time on xxxx 2024 Please take account of time zone differences when submitting your application.
Commonwealth policy entity:	Department of Home Affairs
Administering entity:	Department of Industry, Science and Resources (DISR)
Enquiries:	If you have any questions, contact us on 13 28 46
Date guidelines released:	[dd mmmm yyyy]
Type of grant opportunity:	Open competitive

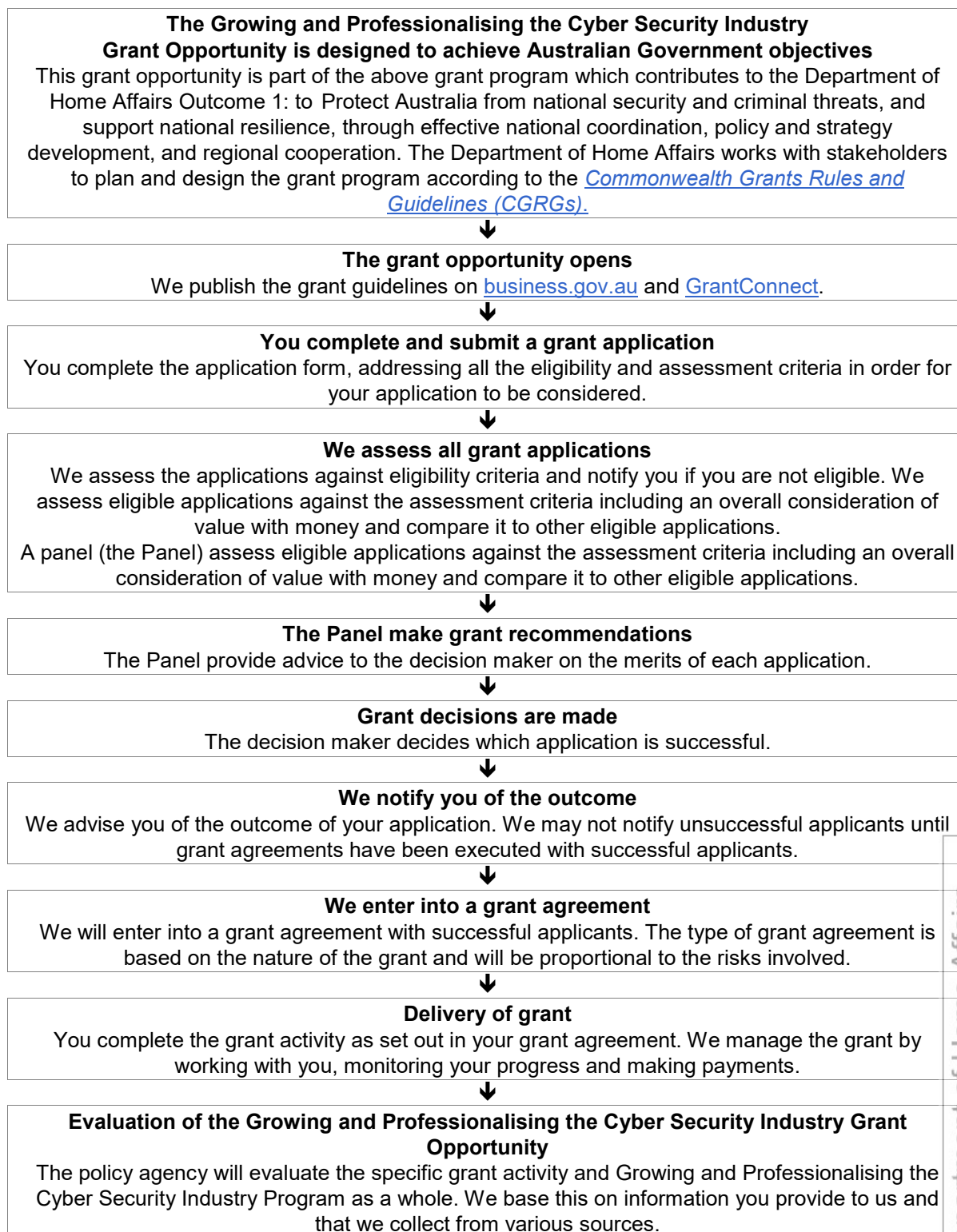
Released by Department of Home Affairs
under the Freedom of Information Act 1982

Contents

1. Growing and Professionalising the Cyber Security Industry Program processes.....	4
1.1. Introduction	5
2. About the grant program.....	5
3. Grant amount and grant period	6
3.1. Grants available	6
3.2. Project period	6
4. Eligibility criteria	6
4.1. Who is eligible to apply for a grant?.....	6
4.2. Who is not eligible to apply for a grant?.....	7
5. What the grant money can be used for	7
5.1. Eligible grant activities	7
5.2. Eligible locations	7
5.3. Eligible expenditure.....	8
5.4. What the grant money cannot be used for.....	8
6. The assessment criteria.....	9
6.1. Assessment criterion 1.....	9
6.2. Assessment criterion 2.....	9
6.3. Assessment criterion 3.....	10
6.4. Assessment criterion 4.....	10
7. How to apply.....	10
7.1. Attachments to the application.....	11
7.2. Joint (consortia) applications	11
7.3. Timing of grant opportunity processes.....	12
7.4. Questions during the application process.....	12
8. The grant selection process	12
8.1. Assessment of grant applications	12
8.2. Who will assess applications?	13
8.3. Who will approve grants?	13
9. Notification of application outcomes.....	14
9.1. Feedback on your application.....	14
10. Successful grant applications	14
10.1. The grant agreement	14
10.2. Specific legislation, policies and industry standards.....	14
10.2.1. Child safety requirements	14
10.3. How we pay the grant	15
10.4. Grant Payments and GST	15
11. Announcement of grants	15
12. How we monitor your grant activity.....	16

12.1.	Keeping us informed	16
12.2.	Reporting	16
12.2.1.	Progress reports.....	16
12.2.2.	Ad-hoc reports.....	16
12.2.3.	End of project report	17
12.3.	Audited financial acquittal report.....	17
12.4.	Grant agreement variations	17
12.5.	Compliance visits	17
12.6.	Record keeping.....	17
12.7.	Evaluation	18
12.8.	Acknowledgement.....	18
13.	Probity.....	18
13.1.	Enquiries and feedback	18
13.2.	Conflicts of interest	19
13.3.	Privacy	19
13.4.	Confidential information	20
13.5.	Freedom of information.....	20
14.	Glossary.....	22

1. Growing and Professionalising the Cyber Security Industry Program processes


 Released by Department of Home Affairs
under the Freedom of Information Act 1982

1.1. Introduction

These guidelines contain information for the Growing and Professionalising the Cyber Security Industry grant program.

This document sets out:

- the purpose of the grant program/grant opportunity
- the eligibility and assessment criteria
- how we consider and assess grant applications
- how we notify applicants and enter into grant agreements with grantees
- how we monitor and evaluate grantees' performance
- responsibilities and expectations in relation to the opportunity.

This grant opportunity and process will be administered by the Department of Industry, Science and Resources (the department/DISR) on behalf of the Department of Home Affairs.

We have defined key terms used in these guidelines in the glossary at section 14.

You should read this document carefully before you fill out an application.

2. About the grant program

The Growing and Professionalising the Cyber Security Industry Program (the Program) was announced as part of the 2023-2030 Australian Cyber Security Strategy (the Strategy).

In response to industry calls for greater clarity around how cyber security qualifications and skills map to industry requirements, this grant program will provide \$1.9 million in funding to design, promote and pilot a professionalisation scheme for Australia's cyber security workforce. Funding will be provided over 2 years from 2024-25 to 2025-26.

The scheme will provide employers and businesses with assurance that the cyber security professionals they hire have the necessary skills and training. It will support applicants to enter and progress within the sector through horizontal and vertical avenues.

The scheme will engage with existing skills frameworks and professional accreditation streams to maximise interoperability with industry and across jurisdictions. It will foster growth of the domestic cyber workforce and remove barriers to entry for job seekers, existing professionals, and minority groups. A consultative, industry-led approach will inform design.

The objectives of the grant program are to:

- establish a pilot industry-led cyber security professionalisation scheme
- provide clear career, skills and education pathways for cyber security professionals, and quality assurance for employers about professional qualifications and cyber security experience of job seekers
- reduce barriers to entry into the cyber industry
- attract and retain diverse talent, and foster inclusive cultures
- enhance domestic cyber capabilities through professionalising the cyber security workforce
- increase industry and business confidence in Australia's cyber security workforce.

The intended outcomes of the program are:

- a pilot Cyber Security Professionalisation Scheme and standards developed in collaboration with industry

- a pilot Cyber Security Professionalisation Scheme that provides clear career, skills and education pathways for workers in, and those seeking to enter, the cyber security workforce
- guidance for employers and employees regarding skills expectations for accredited professionals
- a pilot of the professionalisation scheme and evaluation
- a plan to scale the scheme after the pilot that includes:
 - a strategy to increase industry uptake and participation in the scheme
 - an independent funding mechanism to sustain the program following the pilot, that doesn't introduce further barriers to entry into the cyber industry.

We administer the program according to the [Commonwealth Grants Rules and Guidelines](#) (CGRGs)¹.

3. Grant amount and grant period

3.1. Grants available

The Australian Government has announced a total of \$1.9 million over 2 years for the program.

The maximum grant amount is \$1.9 million.

The grant amount will be 100% per cent of eligible expenditure.

You are responsible for the remaining eligible and ineligible project costs.

3.2. Project period

You must complete your project by June 2026.

4. Eligibility criteria

We cannot consider your application if you do not satisfy all eligibility criteria.

4.1. Who is eligible to apply for a grant?

To be eligible you must:

- have an Australian Business Number (ABN)
- be registered for the Goods and Services Tax (GST)
- be located in Australia
- have an account with an Australian financial institution
- an entity, incorporated in Australia

Joint applications are acceptable, provided you have a lead organisation who is the main driver of the project and is eligible to apply. For further information on joint applications, refer to section 7.2.

¹ <https://www.finance.gov.au/government/commonwealth-grants/commonwealth-grants-rules-guidelines>

4.2. Who is not eligible to apply for a grant?

You are not eligible to apply if you are:

- an organisation, or your project partner is an organisation, included on the [National Redress Scheme's website](#) on the list of 'Institutions that have not joined or signified their intent to join the Scheme'
- an employer of 100 or more employees that has [not complied](#) with the *Workplace Gender Equality Act (2012)*.
- an individual
- a partnership
- an unincorporated association
- any organisation not included in section 4.1
- a trust (however, an incorporated trustee may apply on behalf of a trust)
- a Commonwealth, state, territory or local government body (including government business enterprises)
- a non-corporate Commonwealth entity.

5. What the grant money can be used for

5.1. Eligible grant activities

To be eligible your project must address the objectives and outcomes listed at Section 2. Eligible activities must directly relate to the project and must include:

- the development and delivery of the pilot cyber security professionalisation scheme
- the development of career, skills and education pathways for cyber security professionals
- the establishment and involvement of an industry led co-design team/mechanism, or the involvement of an existing consortium of leading cyber industry representatives
- research of comparable schemes internationally and in comparable industries
- conducting, monitoring and evaluating the pilot scheme
- a strategy for how the scheme will be expanded nationally and become self-sustaining at the conclusion of the government funding period.

Your grant activities must also incorporate existing skills and experience from across the cyber workforce, including technical, non-technical and transferable skills that will foster growth and innovation of the industry.

You must consider how the scheme could align with:

- international best practice skills frameworks (refer to the glossary for examples)
- existing professional accreditation schemes (refer to the glossary for examples)
- [the Australian Universities Accord Final Report](#)

We may also approve other activities. Any additional activities must be in line with objectives and outcomes in section 2.

5.2. Eligible locations

Your project can include activities at different locations, as long as they are all in Australia.

5.3. Eligible expenditure

You can only spend the grant on eligible expenditure you have incurred on an agreed project as defined in your grant agreement.

Eligible expenditure items are:

- labour expenditure
- labour on-costs and administrative overhead (up to 30 per cent of labour costs)
- project management activities
- contract expenditure (cost of any agreed project activities that you contract others to do)
- travel (up to 5 per cent of eligible expenditure)
- purchase of computers, ICT software and hardware directly related to the project, including software licencing and subscription fees
- staff training that directly supports the achievement of project outcomes
- promotional activities to support the rollout of the scheme
- establishment costs including legal fees and registration fees
- the cost of an independent audit of project expenditure up to a maximum of 1 per cent of total eligible project expenditure.

We may update the guidance on eligible and ineligible expenditure from time to time. If your application is successful, the version in place when you submitted your application applies to your project.

If your application is successful, we may ask you to verify project costs that you provided in your application. You may need to provide evidence such as quotes for major costs.

Not all expenditure on your project may be eligible for grant funding. The program delegate who is a manager within the department with responsibility for administering the program makes the final decision on what is eligible expenditure and may give additional guidance on eligible expenditure if required.

To be eligible, expenditure must:

- be a direct cost of the project
- be incurred by you for required project audit activities.

You must incur the project expenditure between the project start and end date for it to be eligible unless stated otherwise.

You must not commence your project until you execute a grant agreement with the Commonwealth. We are not responsible for any expenditure you incur until a grant agreement is executed. The Commonwealth will not be liable, and should not be held out as being liable, for any activities undertaken before the grant agreement is executed.

5.4. What the grant money cannot be used for

Expenditure items that are not eligible are:

- capital expenditure including the purchase or upgrade to fixed assets, buildings, and vehicles
- routine operational costs such as rent, utilities, communications, consumables and stationary
- equipment hire, unless the equipment is required to deliver or promote the scheme
- costs incurred in the preparation of a grant application or related documentation
- construction/capital works

- delivery of work that does not fall within the scope of this grant program.

6. The assessment criteria

You must address all assessment criteria in your application. We will assess your application based on the weighting given to each criterion.

The application form asks questions that relate to the assessment criteria below. The amount of detail and supporting evidence you provide in your application should be relative to the project size, complexity and grant amount requested. You should provide evidence to support your answers. The application form displays character limits for each response.

We will only award funding to applications that score at least 50 per cent against each assessment criterion.

6.1. Assessment criterion 1

Project alignment with policy intent (program objectives and outcomes) (40 points).

Applicants must demonstrate how they will meet the program objectives and outcomes listed at section 2 of the grant opportunity guidelines.

You must demonstrate this through identifying how your project will:

- design, develop and deliver-a pilot, industry-led, Professionalisation Scheme (this must be addressed in your project plan)
- define clear career, skills and education pathways for cyber security professionals
- provide quality assurance for employers about professional qualifications and cyber security experience of job seekers
- foster growth of the domestic cyber workforce, improve diversity and remove barriers for entry into the workforce for job seekers, existing professionals, and minority groups
- be expanded nationally and the effectiveness evaluated
- transition away from government funding and become self-sustaining without creating further barriers to entry into the cyber industry.

A project plan must be attached to address this criterion and must include implementation methodology, timeframes, budget and risk management (up to ten pages).

When developing your project plan you must:

- consider and leverage existing and ongoing work in the development of skills frameworks and professional accreditation schemes to maximise interoperability and alignment with industry and other jurisdictions
- consider comparable schemes internationally and in comparable industries to ensure best practice
- select relevant industry participants to take part in the pilot, demonstrating their suitability in terms of adequate representation of industry (eg. broad range of skills, industry sectors, mid-career transitioners minority cohorts).

6.2. Assessment criterion 2

Collaborative approach to design and implementation (20 points).

You must demonstrate this through identifying:

- a. your experience developing strategic connections across wide groups of stakeholders and the ability to ensure continued collaboration across diverse industry participants to meet common goals and deliver outcomes
- b. your strategy for collaboration with the Australian cyber security industry and other relevant stakeholders (including the Future Skills Organisation, the Executive Cyber Council Workforce Working Group, accreditation bodies, federal, state and territory governments) to design and deliver the scheme, and how your strategy will align with government priorities, including the recommendations of the Australian Universities Accord Final Report
- c. evidence of planned industry collaboration and support to design and deliver the scheme (new or existing consortiums of leading cyber industry representatives and/or letters of support from peak industry bodies).

6.3. Assessment criterion 3

Knowledge, capability and resources to deliver the project (20 points).

You must demonstrate this through providing:

- a. details of your track record delivering on objectives and performance measures in complex environments, and ability to develop and pilot new schemes which deliver impactful outcomes
- b. details of your understanding of, and/or capacity to obtain data, metrics, and information about the Australian cyber security workforce and professional pathways to inform the development of the scheme
- c. details of your access to personnel with appropriate skills sets, expertise and experience, including management and technical staff (the skills and experience of key personnel must be attached as per 7.1).

6.4. Assessment criterion 4

Pilot promotion, monitoring and evaluation (20 points).

Your application must detail how you will:

- a. promote the scheme in a way that educates industry, supports new starters and those seeking a mid-career transition, and captures parallel industries that rely on cyber-skilled workers
- b. conduct, monitor and evaluate the pilot scheme. The monitoring and evaluation strategy should demonstrate how, at the end of the project you will provide:
 - an assessment of how your project has addressed the gap of a national professionalisation scheme and standard for cyber security professionals
 - an assessment of how your project reduced existing barriers for industry, and barriers to entry for job seekers and cyber professionals
 - an overview of the contribution of the industry consortium to the project, including how their role benefited and enabled the projects' delivery.

7. How to apply

Before applying you should read and understand these guidelines, the sample [application form](#) and the sample [grant agreement](#) published on business.gov.au and GrantConnect.

Applicants should read all eligibility and assessment criteria closely and attach detailed evidence that supports the assessment criteria.

You will need to set up an account to access our online [portal](#). You can only submit an application during a funding round.

To apply, you must:

- complete and submit the application through the online [portal](#)
- provide all the information requested
- address all eligibility and assessment criteria
- include all necessary attachments.

You are responsible for making sure your application is complete and accurate. Giving false or misleading information is a serious offence under the [Criminal Code Act 1995](#). If we consider that you have provided false or misleading information we may not progress your application. If you find an error in your application after submitting it, you should call us immediately on 13 28 46.

After submitting your application, we can contact you for clarification if we find an error or any missing information, including evidence that supports your eligibility/merit. The acceptance of any additional information provided after the submission of your application is at the discretion of the program delegate. Additional information should not materially change your application at the time it was submitted and therefore may be refused if deemed to be purely supplementary.

You can view and print a copy of your submitted application on the portal for your own records.

If you need further guidance around the application process, or if you have any issues with the portal, [contact us](#) at business.gov.au or by calling 13 28 46.

7.1. Attachments to the application

You must provide the following documents with your application:

- a project plan including implementation methodology, timeframes, budget and risk management (up to ten pages)
- skills and experience of key personnel
- evidence of new or existing consortiums of leading cyber industry representatives and/or letters of support from peak industry bodies (up to three letters)
- trust deed (where applicable).

You must attach supporting documentation to the application form in line with the instructions provided within the form. You should only attach requested documents. The total of all attachments cannot exceed 20MB. We will not consider information in attachments that we do not request.

7.2. Joint (consortia) applications

We recognise that some organisations may want to join together as a group to deliver a project. In these circumstances, you must appoint a lead organisation. Only the lead organisation can submit the application form and enter into the grant agreement with the Commonwealth. The application must identify all other members of the proposed group and include a letter of support from each of the project partners. Each letter of support should include:

- details of the project partner
- an overview of how the project partner will work with the lead organisation and any other project partners in the group to successfully complete the project
- an outline of the relevant experience and/or expertise the project partner will bring to the group
- the roles/responsibilities the project partner will undertake, and the resources it will contribute (if any)
- details of a nominated management level contact officer.

You must have a formal arrangement in place with all parties prior to execution of the grant agreement.

7.3. Timing of grant opportunity processes

You can only submit an application between the published opening and closing dates. We cannot accept late applications.

If you are successful, we expect you will be able to commence your project around September 2024.

Table 1: Expected timing for this grant opportunity

Activity	Timeframe
Assessment of applications	4 weeks
Approval and announcement of successful applicants	4 weeks
Negotiations and award of grant agreements	4 weeks
Notification to unsuccessful applicants	2 weeks
Earliest start date of project	November 2024
Project completion date	June 2026

7.4. Questions during the application process

If you have any questions during the application period, [contact us](#) at business.gov.au or by calling 13 28 46.

8. The grant selection process

8.1. Assessment of grant applications

We first review your application against the eligibility criteria.

If eligible, your application will be assessed against the assessment criteria. Only eligible applications will proceed to the assessment stage.

We consider your application on its merits, based on:

- how well it meets the criteria
- how it compares to other applications
- whether it provides value with relevant money.²

When assessing the extent to which the application represents value with relevant money, we will have regard to:

- the overall objective/s of the grant opportunity
- the evidence provided to demonstrate how your project contributes to meeting those objectives
- the relative value of the grant sought
- how the grant activities will target groups or individuals.

² See glossary for an explanation of 'value with money'.

If applications are scored the same, the program delegate will consider value for money and alignment to the program objectives to recommend applications for funding.

We also consider any national interest, financial, legal/regulatory, governance or other issue or risk that we identify during any due diligence process that we conduct in respect of the applicant. This includes its directors, officers, senior managers, key personnel, its related bodies corporate (as defined in the *Corporations Act*) or its application that could bring the Australian Government into disrepute if it were to fund the applicant. Such issues and risks include where we consider that funding the application under this grant opportunity is likely to directly conflict with Australian Government policy. Where possible³, we will provide you with an opportunity to comment on any material risks identified during this due diligence process prior to our determining the extent (if any) to which those issues or risks affect our assessment of the application and, if so, whether they are sufficient to warrant the exclusion of your application from the assessment process.

8.2. Who will assess applications?

We assess your application against the selection (eligibility and merit) criteria.

We refer all eligible applications to a departmental Panel comprised of representatives from the Australian Public Service Commission, the Department of Employment and Workplace Relations, DISR and the Department of Home Affairs. The Panel may seek additional advice from independent technical experts or advisors.

The Panel will assess your application against the assessment criteria and compare it to other eligible applications before recommending which projects to fund. The Panel, and any expert or advisor, will be required to perform their duties in accordance with the CGRGs.

If applications are scored the same, the Panel will consider value for money and alignment to the program objectives to recommend applications for funding.

The Panel may seek additional information about you or your application. They may do this from within the Commonwealth, even if you do not nominate the sources as referees. The Panel may also consider information about you or your application that is available as a result of the due diligence process or through the normal course of business.

8.3. Who will approve grants?

The Deputy Secretary, Cyber and Infrastructure Security, Department of Home Affairs decides which grants to approve taking into account the application assessment and/or the recommendations/advice of the Panel and the availability of grant funds.

The Deputy Secretary's decision is final in all matters, including:

- the grant approval
- the grant funding to be awarded
- any conditions attached to the offer of grant funding.

We cannot review decisions about the merits of your application.

The decision maker will not approve funding if there are insufficient program funds available across relevant financial years for the program.

³ Subject to national security and other considerations.

9. Notification of application outcomes

We will advise you of the outcome of your application in writing. If you are successful, we advise you of any specific conditions attached to the grant.

9.1. Feedback on your application

If you are unsuccessful, we will give you an opportunity to discuss the outcome with us.

10. Successful grant applications

10.1. The grant agreement

You must enter into a legally binding grant agreement with the Commonwealth. Each grant agreement has general terms and conditions that cannot be changed. Sample grant agreements are available on business.gov.au and GrantConnect. The grant agreement has general terms and conditions that cannot be changed. A sample [grant agreement](#) is available on business.gov.au and GrantConnect.

We will manage the grant agreement through the online portal. This includes issuing and executing the grant agreement. Execute means both you and the Commonwealth have accepted the agreement. You must not start any Growing and Professionalising the Cyber Security Industry activities until a grant agreement is executed. We are not responsible for any expenditure you incur and cannot make any payments until a grant agreement is executed.

The approval of your grant may have specific conditions determined by the assessment process or other considerations made by the Minister. We will identify these in the offer of grant funding.

If you enter an agreement under the Growing and Professionalising the Cyber Security Industry Program, you cannot receive other grants for the same activities from other Commonwealth, state or territory granting programs.

The Commonwealth may recover grant funds if there is a breach of the grant agreement.

We will use a standard grant agreement for medium or larger projects where we consider your project to be more complex.

You will have 30 days from the date of a written offer to execute this grant agreement with the Commonwealth. During this time, we will work with you to finalise details.

The offer may lapse if both parties do not sign the grant agreement within this time. Under certain circumstances, we may extend this period. We base the approval of your grant on the information you provide in your application. We will review any required changes to these details to ensure they do not impact the project as approved by the program delegate.

10.2. Specific legislation, policies and industry standards

You must comply with all relevant laws, regulations and Australian Government sanctions in undertaking your project. You must also comply with the specific legislation/policies/industry standards that follow. It is a condition of the grant funding that you meet these requirements. We will include these requirements in your grant agreement.

10.2.1. Child safety requirements

You must comply with all relevant legislation relating to the employment or engagement of anyone working on the project that may interact with children, including all necessary working with children checks.

You must implement the [National Principles for Child Safe Organisations](#)⁴ endorsed by the Commonwealth.

You will need to complete a risk assessment to identify the level of responsibility for children and the level of risk of harm or abuse, and put appropriate strategies in place to manage those risks. You must update this risk assessment at least annually.

You will also need to establish a training and compliance regime to ensure personnel are aware of, and comply with, the risk assessment requirements, relevant legislation including mandatory reporting requirements and the National Principles for Child Safe Organisations.

You will be required to provide an annual statement of compliance with these requirements in relation to working with children.

10.3. How we pay the grant

The grant agreement will state the maximum grant amount we will pay.

We will not exceed the maximum grant amount under any circumstances. If you incur extra costs, you must meet them yourself.

We will make payments according to an agreed schedule set out in the grant agreement. Payments are subject to satisfactory progress on the project.

10.4. Grant Payments and GST

If you are registered for the Goods and Services Tax (GST), where applicable we will add GST to your grant payment and provide you with a recipient created tax invoice. You are required to notify us if your GST registration status changes during the project period. GST does not apply to grant payments to government related entities⁵.

Grants are assessable income for taxation purposes, unless exempted by a taxation law. We recommend you seek independent professional advice on your taxation obligations or seek assistance from the [Australian Taxation Office](#). We do not provide advice on tax.

11. Announcement of grants

If successful, your grant will be listed on the GrantConnect website 21 calendar days after the date of execution.

We will publish non-sensitive details of successful projects on GrantConnect. We are required to do this by the [Commonwealth Grants Rules and Guidelines](#), Section 5.3, We may also publish this information on business.gov.au. This information may include:

- name of your organisation
- title of the project
- description of the project and its aims
- amount of grant funding awarded
- Australian Business Number
- business location
- your organisation's industry sector.

⁴ <https://www.humanrights.gov.au/our-work/childrens-rights/national-principles-child-safe-organisations>

⁵ See Australian Taxation Office ruling GSTR 2012/2 available at ato.gov.au

12. How we monitor your grant activity

12.1. Keeping us informed

You should let us know if anything is likely to affect your project or organisation.

We need to know of any key changes to your organisation or its business activities, particularly if they affect your ability to complete your project, carry on business and pay debts due.

You must also inform us of any changes to your:

- name
- addresses
- nominated contact details
- bank account details.

If you become aware of a breach of terms and conditions under the grant agreement, you must contact us immediately.

You must notify us of events relating to your project and provide an opportunity for the Minister or their representative to attend.

12.2. Reporting

You must submit reports in line with the grant agreement. We will provide the requirements for these reports as appendices in the grant agreement. We will remind you of your reporting obligations before a report is due. We will expect you to report on:

- progress against agreed project milestones and outcomes
- project expenditure, including expenditure of grant funds
- contributions of participants directly related to the project.

The amount of detail you provide in your reports should be relative to the project size, complexity and grant amount.

We will monitor the progress of your project by assessing reports you submit and may conduct site visits to confirm details of your reports if necessary. Occasionally we may need to re-examine claims, seek further information or request an independent audit of claims and payments.

12.2.1. Progress reports

Progress reports must:

- include details of your progress towards completion of agreed project activities
- show the total eligible expenditure incurred to date
- include evidence of expenditure
- be submitted by the report due date (you can submit reports ahead of time if you have completed relevant project activities).

We will only make grant payments when we receive satisfactory progress reports.

You must discuss any project or milestone reporting delays with us as soon as you become aware of them.

12.2.2. Ad-hoc reports

We may ask you for ad-hoc reports on your project. This may be to provide an update on progress, or any significant delays or difficulties in completing the project.

12.2.3. End of project report

When you complete the project, you must submit an end of project report.

End of project reports must:

- include the agreed evidence as specified in the grant agreement
- identify the total eligible expenditure incurred for the project
- include a declaration that the grant money was spent in accordance with the grant agreement and to report on any underspends of the grant money
- be submitted by the report due date.

12.3. Audited financial acquittal report

We will ask you to provide an independent audit report. An audit report will verify that you spent the grant in accordance with the grant agreement. The audit report requires you to prepare a statement of grant income and expenditure. The report template is available on business.gov.au and GrantConnect.

12.4. Grant agreement variations

We recognise that unexpected events may affect project progress. In these circumstances, you can request a variation to your grant agreement, including:

- changing project milestones
- extending the timeframe for completing the project (to be within the maximum project time allowed in the program guidelines)
- changing project activities.

The program does not allow for an increase of grant funds.

If you want to propose changes to the grant agreement, you must put them in writing before the project grant agreement end date. You can submit a variation request via our online portal.

If a delay in the project causes milestone achievement and payment dates to move to a different financial year, you will need a variation to the grant agreement. We can only move funds between financial years if there is enough program funding in the relevant year to allow for the revised payment schedule. If we cannot move the funds, you may lose some grant funding.

You should not assume that a variation request will be successful. We will consider your request based on factors such as:

- how it affects the project outcome
- consistency with the program policy objective, grant opportunity guidelines and any relevant policies of the department
- changes to the timing of grant payments
- availability of program funds.

12.5. Compliance visits

We may visit you during the project period, or at the completion of your project to review your compliance with the grant agreement. For large or complex projects, we may visit you after you finish your project. We will provide you with reasonable notice of any compliance visit.

12.6. Record keeping

We may also inspect the records you are required to keep under the grant agreement.

12.7. Evaluation

The Department of Home Affairs will evaluate the grant program to measure how well the outcomes and objectives have been achieved. We may use information from your application and project reports for this purpose. We may also interview you or ask you for more information to help us understand how the grant impacted you and to evaluate how effective the program was in achieving its outcomes.

We may contact you up to two years after you finish your project for more information to assist with this evaluation.

12.8. Acknowledgement

If you make a public statement about a project funded under the program, including in a brochure or publication, you must acknowledge the grant by using the following:

‘This project received grant funding from the Australian Government.’

If you erect signage in relation to the project, the signage must contain an acknowledgement of the grant.

13. Probity

We will make sure that the grant opportunity process is fair, according to the published guidelines, incorporates appropriate safeguards against fraud, unlawful activities and other inappropriate conduct and is consistent with the CGRGs.

These guidelines may be changed from time-to-time by DISR. When this happens, the revised guidelines will be published on GrantConnect.

13.1. Enquiries and feedback

For further information or clarification, you can contact us on 13 28 46 or by [web chat](#) or through our [online enquiry form](#) on business.gov.au.

We may publish answers to your questions on our website as Frequently Asked Questions.

Our [Customer Service Charter](#) is available at business.gov.au. We use customer satisfaction surveys to improve our business operations and service.

If you have a complaint, call us on 13 28 46. We will refer your complaint to the appropriate manager.

If you are not satisfied with the way we handle your complaint, you can contact:

General Manager
External Programs Branch
Business Grants Hub and Integrity Division
Department of Industry, Science and Resources
GPO Box 2013
CANBERRA ACT 2601

You can also contact the [Commonwealth Ombudsman](#) with your complaint (call 1300 362 072). There is no fee for making a complaint, and the Ombudsman may conduct an independent investigation.

13.2. Conflicts of interest

Any conflicts of interest could affect the performance of the Growing and Professionalising the Cyber Security Industry program. There may be a conflict of interest, or perceived conflict of interest, if our staff, any member of a panel or advisor and/or you or any of your personnel:

- has a professional, commercial or personal relationship with a party who is able to influence the application selection process, such as an Australian Government officer or member of an external panel
- has a relationship with or interest in, an organisation, which is likely to interfere with or restrict the applicants from carrying out the proposed activities fairly and independently or
- has a relationship with, or interest in, an organisation from which they will receive personal gain because the organisation receives a grant under the grant program/grant opportunity.

As part of your application, we will ask you to declare any perceived or existing conflicts of interests or confirm that, to the best of your knowledge, there is no conflict of interest.

If you later identify an actual, apparent, or perceived conflict of interest, you must inform us in writing immediately.

Conflicts of interest for Australian Government staff are handled as set out in the Australian [Public Service Code of Conduct \(Section 13\(7\)\)](#) of the [Public Service Act 1999](#). Panel members and other officials including the decision maker must also declare any conflicts of interest.

We publish our [conflict of interest policy](#)⁶ on the department's website. The Commonwealth policy entity also publishes a conflict of interest policy on its website.

13.3. Privacy

Unless the information you provide to us is:

- confidential information as per below, or
- personal information as per below.

we may share the information with other government agencies for a relevant Commonwealth purpose such as:

- to improve the effective administration, monitoring and evaluation of Australian Government programs
- for research
- to announce the awarding of grants.

We must treat your personal information according to the Australian Privacy Principles (APPs) and the *Privacy Act 1988* (Cth). This includes letting you know:

- what personal information we collect
- why we collect your personal information
- to whom we give your personal information.

We may give the personal information we collect from you to our employees and contractors, the Panel, and other Commonwealth employees and contractors, so we can:

- manage the program
- research, assess, monitor and analyse our programs and activities.

⁶ <https://www.industry.gov.au/publications/conflict-interest-policy>

We, or the Minister, may:

- announce the names of successful applicants to the public
- publish personal information on the department's websites.

You may read our [Privacy Policy](#)⁷ on the department's website for more information on:

- what is personal information
- how we collect, use, disclose and store your personal information
- how you can access and correct your personal information.

13.4. Confidential information

Other than information available in the public domain, you agree not to disclose to any person, other than us, any confidential information relating to the grant application and/or agreement, without our prior written approval. The obligation will not be breached where you are required by law, Parliament or a stock exchange to disclose the relevant information or where the relevant information is publicly available (other than through breach of a confidentiality or non-disclosure obligation).

We may at any time, require you to arrange for you; or your employees, agents or subcontractors to give a written undertaking relating to nondisclosure of our confidential information in a form we consider acceptable.

We will treat the information you give us as sensitive and therefore confidential if it meets all of the following conditions:

- you clearly identify the information as confidential and explain why we should treat it as confidential
- the information is commercially sensitive
- disclosing the information would cause unreasonable harm to you or someone else
- you provide the information with an understanding that it will stay confidential.

We may disclose confidential information:

- to the Panel and our Commonwealth employees and contractors, to help us manage the program effectively
- to the Auditor-General, Ombudsman or Privacy Commissioner
- to the responsible Minister or Assistant Minister
- to a House or a Committee of the Australian Parliament.

We may also disclose confidential information if:

- we are required or authorised by law to disclose it
- you agree to the information being disclosed, or
- someone other than us has made the confidential information public.

13.5. Freedom of information

All documents in the possession of the Australian Government, including those about the program, are subject to the *Freedom of Information Act 1982* (Cth) (FOI Act).

The purpose of the FOI Act is to give members of the public rights of access to information held by the Australian Government and its entities. Under the FOI Act, members of the public can seek

⁷ <https://www.industry.gov.au/data-and-publications/privacy-policy>

access to documents held by the Australian Government. This right of access is limited only by the exceptions and exemptions necessary to protect essential public interests and private and business affairs of persons in respect of whom the information relates.

If someone requests a document under the FOI Act, we will release it (though we may need to consult with you and/or other parties first) unless it meets one of the exemptions set out in the FOI Act.

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

14. Glossary

Term	Definition
administering entity	When an entity that is not responsible for the policy, is responsible for the administration of part or all of the grant administration processes.
application form	The document issued by the program delegate that applicants use to apply for funding under the program.
assessment criteria	The specified principles or standards, against which applications will be judged. These criteria are also used to assess the merits of proposals and, in the case of a competitive grant opportunity, to determine application ranking.
<u>Commonwealth Grants Rules and Guidelines (CGRGs)</u>	Establish the overarching Commonwealth grants policy framework and articulate the expectations for all non-corporate Commonwealth entities in relation to grants administration. Under this overarching framework, non-corporate Commonwealth entities undertake grants administration based on the mandatory requirements and key principles of grants administration.
completion date	The expected date that the grant activity must be completed and the grant spent by.
consortium	A group of organisations or individuals with the objective of sharing resources for achieving a common goal.
date of effect	Can be the date on which a grant agreement is signed or a specified starting date. Where there is no grant agreement, entities must publish information on individual grants as soon as practicable.
Department	The Department of Industry, Science and Resources.
decision maker	The person who makes a decision to award a grant. For the program, the decision maker is the Deputy Secretary, Cyber and Infrastructure Security, Department of Home Affairs.
The Panel	The body established by the Department of Home Affairs comprising representatives from the Australian Public Service Commission, Department of Employment and Workplace Relations, DISR and the Department of Home Affairs, and other relevant departments. The Panel will consider and assess eligible applications and make recommendations to the decision maker for funding under the program.
eligible activities	The activities undertaken by a grantee in relation to a project that are eligible for funding support as set out in 5.1.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Term	Definition
eligible application	An application or proposal for grant funding under the program that the program delegate has determined is eligible for assessment in accordance with these guidelines.
eligibility criteria	Refer to the mandatory criteria which must be met to qualify for a grant. Assessment criteria may apply in addition to eligibility criteria.
eligible expenditure	The expenditure incurred by a grantee on a project and which is eligible for funding support as set out in 5.3.
General Manager	Position title for Senior Executive Service level staff within DISR.
grant	For the purposes of the CGRGs, a 'grant' is an arrangement for the provision of financial assistance by the Commonwealth or on behalf of the Commonwealth: a. under which relevant money⁸ or other Consolidated Revenue Fund (CRF) money⁹ is to be paid to a grantee other than the Commonwealth; and b. which is intended to help address one or more of the Australian Government's policy outcomes while assisting the grantee achieve its objectives.
grant activity/activities	Refers to the project/tasks/services that the grantee is required to undertake.
grant agreement	A legally binding contract that sets out the relationship between the Commonwealth and a grantee for the grant funding and specifies the details of the grant.
grant funding or grant funds	The funding made available by the Commonwealth to grantees under the program.
grant opportunity	Refers to the specific grant round or process where a Commonwealth grant is made available to potential grantees. Grant opportunities may be open or targeted and will reflect the relevant grant selection process.
grant program	A 'program' carries its natural meaning and is intended to cover a potentially wide range of related activities aimed at achieving government policy outcomes. A grant program is a group of one or more grant opportunities under a single Portfolio Budget Statement Program.

⁸ Relevant money is defined in the PGPA Act. See section 8, Dictionary.

⁹ Other CRF money is defined in the PGPA Act. See section 105, Rules in relation to other CRF money.

Term	Definition
GrantConnect	The Australian Government's whole-of-government grants information system, which centralises the publication and reporting of Commonwealth grants in accordance with the CGRGs.
grantee	The individual/organisation which has been selected to receive a grant.
international best practice skills frameworks	Such as the Skills Framework for the Information Age (SFIA), National Initiative for Cybersecurity Education (NICE), the Cyber Security Body of Knowledge (CyBok), Chartered Institute of Information Security (CIIISec).
Minister	The Commonwealth Minister for Home Affairs
personal information	Has the same meaning as in the <i>Privacy Act 1988</i> (Cth) which is: Information or an opinion about an identified individual, or an individual who is reasonably identifiable: a. whether the information or opinion is true or not; and b. whether the information or opinion is recorded in a material form or not.
professional accreditation schemes	Such as the International Information System Security Certification Consortium (ISC2), Information Systems Audit and Control Association (ISACA), Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM).
program delegate	A manager within the department with responsibility for administering the program.
grant assessment delegate	A manager within the department with responsibility for administering the program.
program funding or program funds	The funding made available by the Commonwealth for the program.
project	A project described in an application for grant funding under the program.
selection criteria	Comprises of eligibility criteria and assessment criteria.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Term	Definition
value with money	Value with money in this document refers to ‘value with relevant money’ which is a judgement based on the grant proposal representing an efficient, effective, economical and ethical use of public resources and determined from a variety of considerations. When administering a grant opportunity, an official should consider the relevant financial and non-financial costs and benefits of each proposal including, but not limited to: ▪ the quality of the project proposal and activities; ▪ fitness for purpose of the proposal in contributing to government objectives; ▪ that the absence of a grant is likely to prevent the grantee and government’s outcomes being achieved; and ▪ the potential grantee’s relevant experience and performance history.



Australian Government

Department of Industry, Science and Resources

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

s. 47(1)(b), s. 47E(d)

s. 47(1)(b), s. 47E(d)

s. 47(1)(b), s. 47E(d)

s. 47(1)(b), s. 47E(d)

s. 47(1)(b), s. 47E(d)

s. 47(1)(b), s. 47E(d)

S. 42(1)

S. 42(1)

S. 42(1)

s. 42(1)



The Hon Tony Burke MP
Minister for Home Affairs
Minister for Immigration and Multicultural Affairs
Minister for Cyber Security
Minister for the Arts
Leader of the House

Ref No: MS24-001013

Senator the Hon Katy Gallagher
Minister for Finance
Parliament House
CANBERRA ACT 2600

Dear Minister

I write to seek your agreement to publically release the *Growing and Professionalising the Cyber Security Industry Program Grant Opportunity Guidelines* (the Guidelines).

In accordance with Estimates Memorandum 2018/39, your approval for the Guidelines (**Attachment A**) is sought on the basis that the program is rated to be medium risk (**Attachment B** refers).

The Department of Finance, in consultation with the Department of the Prime Minister and Cabinet (PM&C), determines the overall program risk. The assessment is based on an analysis of the constitutional, legislative and implementation risks. The overall program risk rating aligns with the highest risk rating across the three risk categories. The medium risk rating for this Grant

s. 42(1)

s. 42(1) (**Attachment B** refers).

s. 42(1)

On 4 April 2024, the former Minister for Home Affairs, the Hon Clare O'Neil MP, wrote to you requesting inclusion of a proposed item in *Schedule 1AB to the Financial Framework (Supplementary Powers) Regulations 1997* (FF(SP) Regulations) s. 42(1)

s. 42(1) Thank you for agreeing to this approach. On 9 May 2024, the Federal Executive Council made the amendment to the FF(SP) Regulations s. 42(1)

s. 42(1)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

s. 42(1)

The Department of Finance and PM&C agree the medium risk rating applies to this Grant. As programs with agreed risk ratings do not require Expenditure Review Committee consideration, with your agreement I would like to approve the guidelines for publication on 6 December 2024.

I am seeking your agreement to release the Guidelines (**Attachment A**). The related risk assessment is also attached for your consideration (**Attachment B**).

Thank you for your attention to this matter.

Yours sincerely



TONY BURKE

11 / 11 / 2024

Encl:

- A. Growing and Professionalising the Cyber Security Industry Program Grant Guidelines
- B. Program guidelines self-assessment risk analysis - Growing and Professionalising the Cyber Security Industry

s. 42(1)

Official Sensitive | Legal Privilege

**Senator the Hon Katy Gallagher**

Minister for Finance
Minister for Women
Minister for the Public Service
Senator for the Australian Capital Territory

REF: MC24-004210

The Hon Tony Burke MP
Minister for Cyber Security
Parliament House
CANBERRA ACT 2600

Dear Minister *Tony*

Thank you for your letter of 11 November 2024, seeking agreement to release the Growing and Professionalising the Cyber Security Industry Grant Opportunity Guidelines (Guidelines).

My department and the Department of the Prime Minister and Cabinet have agreed a medium risk rating is appropriate for the Guidelines, s. 42(1)

s. 42(1) I understand a new item was added in May 2024 to the *Financial Framework (Supplementary Powers) Regulation 1997*, s. 42(1)

I am advised your department has established controls in place to mitigate implementation risks in relation to the program. I acknowledge these and note that mitigations are important in ensuring the grant activities align with the Commonwealth's legislative and constitutional powers.

As you are aware, new requirements for the review and release of grant opportunity guidelines set out in Estimates Memorandum 2024/36 commenced on 21 October 2024 under which you can agree to the release of medium risk Guidelines where any reasonable mitigations have been implemented or where no such mitigations are available.

Yours sincerely

Katy Gallagher
Katy Gallagher

27 NOV 2024