



Australian Government

Commonwealth Contract – Services

Reference ID: PRI-00004515

Customer

Customer Name:	Department of Industry, Science, Energy and Resources
Customer ABN:	74 599 608 295
Address:	Department of Industry, Science, Energy and Resources GPO Box 2013 Canberra ACT 2601

Supplier

Full Name of the Legal Entity:	AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED
Supplier ABN:	73 616 231 451
Address:	Unit 2, Level 4 1 Hobart Place Canberra City ACT 2600

Statement of Work

C.A.1 Key Events and Dates

This Contract commences on the Contract Start Date or the date this Contract is executed, whichever is the latter, and continues for the Contract Term unless:

- a) it is terminated earlier; or
- b) the Customer exercises the Contract Extension Option, in which case this Contract will continue until the end of the extended time (unless it is terminated earlier).

Event	Details
Contract Start Date:	Upon contract execution
Contract Term:	This Contract will terminate on Thursday, 30 June 2022.
Contract Extension Option:	This Contract includes the following extension option(s): Up to an additional 12 months of services.

C.A.2 The Requirement

Background

This project is an initiative under the Australian Government's Cyber Security National Workforce Growth Program. This Program is designed to develop the cyber security skills required now, while creating a pipeline of skilled Australians going forward.

Requirement

The Department of Industry, Science, Energy and Resources (the Customer) has sought expertise to develop or expand a forecasting methodology and model for analysing the Australian cyber security workforce and skills shortages in real-time and to provide regular data reporting to the Customer. This solution would be publically available to enable industry, education, government and the broader Australian community to access this information.

The project aims to strengthen cyber security skills forecasting, labour force and workforce demand data to better understand the current environment and inform future government policies. The data underpinning this work will feed into, or draw from, other agencies' (for example, the Australian Bureau of Statistics; or National Skills Commission; or Department of Education, Skills and Employment) data initiatives and sources as much as possible to minimise duplication and embed long term solutions to data gaps.

Services to be delivered by the Supplier

Deliverable One: Summary Report

1. A comprehensive outline (as a Table of Contents) will be provided which demonstrates the proposed summary report on the state of cyber security workforce and skills shortages in Australia.
2. A written summary report in an agreed format that outlines the current state of Australia's cyber security workforce and skills and capabilities. This includes:
 - a. Definition of the Australian cyber security workforce, including cyber security-related activities which are part of the Australian digital economy.
 - b. Detailed information on data points and sources available for emerging areas of interest in workforce skills and shortages in Australia and internationally and consideration of any data collection and analysis challenges and how these can be effectively addressed.
 - c. Information on the current number of Australians employed in the cyber security workforce, mapping these to both ANZSIC (division) and ANZSCO (code), disaggregating this data by age, gender, geographic location (State/Territory) and average salary where possible.
 - d. An outline of existing advertised job vacancies, at the time of writing, according to both geographic location (State/Territory) and area of specialisation, mapped to the AustCyber-endorsed US National Initiative for Cybersecurity Education's (NICE) Workforce Framework.
 - e. Summary of the most common cyber security qualifications in the Australian labour market, and specifically those that enable higher rates of mobility.
 - f. Detailed glossary of terms.
 - g. Appendix of all data sources, including annotated bibliography summarising variables of data sources referenced and identified data gaps.
 - h. Report information will leverage the NICE framework to frame occupations and job roles and enable international comparison of performance. In conducting this analysis, an inclusion of a comparative overview for the United States, United Kingdom, New Zealand, and Germany; countries where baseline data exists will occur, enabling some comparisons to be made (for example, in areas such as met, oversupply, or shortage).
3. A co-design workshop to be convened to support Supplier and Customer collaboration to shape inputs, definitions and subsequent forecasting model.

Deliverable Two: Forecasting Model

4. The Supplier will significantly augment and improve its existing platform, CyberSeek in response to the requirement to "develop a new model, or configure an existing model, that can provide current and

Commonwealth Contract – Services

forecasting data on cyber security workforce and skills and capability supply, including oversupply and shortages, to enable the Customer and broader stakeholders to better understand Australia's position and how it compares internationally".

5. The Supplier will deliver:
 - a. Supply and demand data - including education and job titles – with reference to education types, certifications, geography of roles (states/territories), ANZSIC Division of roles advertised, ANZSCO code of roles. This will be presented visually, and available, ultimately, to users by time-lapse, to visualise supply and demand trends over time.
 - b. Updated cross-referencing with revised ANZSCO occupations (as available, currently scheduled for November 2021).
 - c. Macro-economic trends (general rates of employment, reported economic growth, including by State/ Territory/ Commonwealth).
 - d. Applicable government and industry policy initiatives (by State/ Territory/ Commonwealth), with specific reference to employment, skills and training for cyber security.
 - e. An atlas of data derived from published international sources, including industry, academic and government reports, on cyber security skills and employment. Initially, this will focus on comparative jurisdictions such as the United Kingdom, United States and New Zealand.
6. The Customer and Supplier will continue to collaborate on specific data outputs and availability of these throughout the course of the contract term which may include:

Baseline Data

a) Australian workforce:

- i. Data on the cyber security sector workforce, including, for example breakdown by gender, neurodiversity (if known), age distribution, geography (states/territories), average salary
- ii. Baseline data of cyber security professionals in each ANZSIC Division (by above variables (for example manufacturing; construction; agriculture; accommodation and food services; retail trade), ANZSCO code (categorise role), and product/service provision
- iii. International comparisons of the Australian workforce and skills supply (shortages, met, oversupply)

b) Cyber security workforce recruitment:

- i. Total cyber security job openings, with breakdown for example by employment type (full-time, part-time), geography (states/territories), ANZSIC Division (categorise sector), ANZSCO code (categorise role)
- ii. Total job openings, with breakdown for example by requested education level; most sought after certifications requested by employers; most sought after skills requested
- iii. Breakdown of job openings by cyber security job titles including information on most sought after), and commensurate salary
- iv. Time to recruit
- v. Failure rates

c) Cyber security related education:

- i. Enrolments by type of institution, for example VET, Universities, private institutions
- ii. Number of graduates
- iii. Educational institutions and courses
- iv. Number and type of certification holders
- v. Linkages between certifications and cyber security jobs via common skills

Commonwealth Contract – Services

Forecasting Data

d) Cyber security workforce and skills forecast:

- i. Supply/Demand of cyber security workers and skills and capabilities, including, for example breakdown by gender, neurodiversity (if known), age distribution, geography (states/territories), average salary
- ii. Growth rates – including education and job titles – including breakdown for example by education types, certifications, geography of roles (states/territories), ANZSIC Division of roles advertised; ANZSCO code of roles
- iii. Career transition trends, for example which professions/industries are workers transitioning from and into cyber security

e) Summary information on factors impacting workforce and skills forecasts:

- i. Economic shifts
- ii. Government policy and program impacts
- iii. International influences
- iv. Cyber Security sector initiatives or programs led by industry
- i. Other factors affecting potential skilled workers for now or the future, for example:
 - K to 12 education, Vocational or Tertiary education
 - Training opportunities for graduates or workers more broadly
 - Unemployed persons
 - Employed persons not in cyber security roles (ie. in other sectors)
 - International labour
 - Net loss of workers out of cyber security profession (for example due to retirement)

7. The Supplier will maintain ownership of the model and must retain responsibility for the ongoing maintenance of the model and data.
 - a. The Supplier will involve the Customer in the development and planning processes for a forecasting model, including data points and data sources to be used.
 - b. The Customer may request Government data sources be used in the model. Where this request is made, the Customer will source the data and provide to the Supplier as available. The Customer and Supplier will need to agree on these data sources and ongoing ownership.
8. The outputs of the model will be publically available.
9. The Supplier will provide qualified staff with project management capabilities to meet these requirements.
10. The model will be regularly updated as new or amended data inputs become available.

Data reporting

11. An agreed report template will be developed for routine (quarterly) provision of data to the Customer as well as any ad-hoc reporting that may be required.
12. The Supplier will:
 - a. Work with the Customer to develop this agreed format and frequency for regular data reporting. The Supplier will be most often seeking high quality, low frequency data reports, in recognition that data outputs are subject to the availability and updates of data source inputs. Features may include, but are not limited to, dashboards, heat maps and/or graphical representations.
 - i. The Supplier will work with the Customer on any changes to the agreed format and frequency of reporting where this changes from quarterly reporting.
 - ii. The Supplier will provide data to the Customer in an agreed regular format and frequency beyond the term of this contract at no additional cost.
 - b. Deliver on ad-hoc or bespoke data requests from the Customer which must be delivered in agreed timeframes between the Supplier and Customer.
 - i. The Supplier will not be required to provide ad-hoc or bespoke data to the Customer at no additional cost beyond the term of this contract. The Supplier may provide a quote and following agreement from the Customer, provide an invoice for delivered services.

Commonwealth Contract – Services

13. The Supplier will continue to update its online and public platform as it receives updates or additional data. This will allow more granular and timely trend reporting on the public-instance.
14. AustCyber adheres with all applicable employment laws and maintains a strong focus on ethical, safe and secure supply chain practices. For example, verification of suppliers, according to ownership, operating environment and known past dealings is a key component of all active partnerships we maintain. We also maintain organisational policies in areas such as non-discrimination and employment entitlements.

C.A.2(a) Standards

The Supplier must ensure that any goods and services provided under this Contract comply with all applicable Australian standards (or in its absence an international standard) including any requirements or standards specified in this Statement of Work. If requested by the Customer, the Supplier must enable the Customer, or an independent assessor, to conduct periodic audits to confirm compliance with all applicable Australian or international standards, including, but not limited to, those specified in this Statement of Work.

Web Content Accessibility

As applicable, the Supplier must ensure that any website, associated material and/or online publications (where applicable) complies with the Web Content Accessibility Guidelines available at: <https://www.w3.org/WAI/intro/wcag>.

C.A.2(b) Security Requirements

None Specified

C.A.2(c) Work Health and Safety

Prior to commencement of this Contract, the Customer's Contract Manager and the Supplier's Contract Manager will identify any potential Work Health and Safety issues anticipated to arise during the term of this contract and assign management of each issue identified to the party best able to manage it. The Supplier will provide the Customer with a plan for approval.

Throughout the Contract Term, the Customer and the Supplier will proactively identify and cooperate to manage any Work Health and Safety issues that arise.

C.A.2(d) Delivery and Acceptance

Where the Customer rejects any deliverables under Clause C.C.11 [*Delivery and Acceptance*] the Customer will specify a timeframe in which the Supplier is required to rectify deficiencies, at the Supplier's cost, so that the deliverables meet the requirements of this Contract. The Supplier must comply with any such requirement. Rectified deliverables are subject to acceptance under Clause C.C.11 [*Delivery and Acceptance*].

The Supplier will refund all payments related to the rejected deliverables unless the relevant deliverables are rectified and accepted by the Customer.

If the Supplier is unable to meet the Customer's timeframe, the Customer may terminate this Contract in accordance with Clause C.C.16 [*Termination for Cause*].

Milestone Description	Contact for Delivery	Delivery Location/Email	Due Date
Comprehensive outline (as a Table of Contents) of the proposed summary report on the state of cyber security workforce and skills shortages in Australia delivered	cybersecurity@industry.gov.au	Email	9/07/2021

Commonwealth Contract – Services

Draft project management plan and proposed project plan delivered	cybersecurity@industry.gov.au	Email	16/07/2021
Co-design workshop – summary report	Cyber Security Industry Policy Team	Canberra, contingent on prevailing public health advice. Otherwise videoconference	23/07/2021
Draft summary report delivered	cybersecurity@industry.gov.au	Email	06/08/2021
Forecasting Model demonstration involving the department (and may involve other relevant stakeholders with a vested interest in cyber security workforce and skills forecasting)	Cyber Security Industry Policy Team	Face to face or Video-Conference	To be negotiated between Customer and Supplier
Launch of Forecasting Model	Cyber Security Industry Policy Team	To be confirmed	To be negotiated between Customer and Supplier
Data Reporting Template for agreement	cybersecurity@industry.gov.au	Email	To be negotiated between Customer and Supplier
Ongoing Cyber Security Data Reports at an agreed frequency	cybersecurity@industry.gov.au	Email	To be negotiated between Customer and Supplier

C.A.2(e) Meetings

The Supplier is required to attend meetings as follows:

Meeting Type	Position Required	Frequency	Teleconference/ Onsite	Location
Initial Project Scoping Meeting	Supplier CEO and relevant project management staff	One-off	On-site	To be confirmed based on mutual availability
Progress Meetings	Relevant project management staff	Monthly	Teleconference	n/a
Contract mid-point Meeting	Supplier CEO and relevant project management and technical staff as needed	One-off	On-site	To be confirmed based on mutual availability
End of Project Meeting	Supplier CEO and relevant project management and technical staff as needed	One-off	On-site	To be confirmed based on mutual availability

C.A.2(f) Facilities and Assistance Offered by the Customer

The Customer will provide assistance to the Supplier as requested and mutually agreed to ensure the forecasting model and subsequent data assets are fit-for-purpose.

The Customer will not provide facilities.

C.A.2(g) Customer Material

The Customer will provide:

1. Any data sources available that can be shared with the Supplier;
2. Any other materials to support the Suppliers development of the model and data.

C.A.2(h) Conflicts of Interest

The Supplier has declared that it has no actual, perceived or potential conflicts of interest relevant to the performance of its obligations under this Contract.

C.A.2(i) Public Interest Disclosure

For information about how to make a public interest disclosure, please refer to the information provided on the department's website - <https://www.industry.gov.au/about-us/what-we-do/public-interest-disclosure>.

C.A.2(j) Complaints Handling

Any complaints relating to this procurement should sent to: Procurement.Complaints@industry.gov.au.

Commonwealth Contract – Services

C.A.3 Contract Price

The maximum Contract Price inclusive of GST and all taxes and charges will not exceed **s47(1)(b)** as set out below.

Fixed Price (including all expenses)

Due Date	Milestone Description	Total Price GST Exclusive	GST Component	Total Price GST Inclusive
06/08/2021	Deliverable One: (Including outline, project plan and written summary report)	s47(1)(b)	s47(1)(b)	s47(1)(b)
Contract execution	Deliverable Two: (Commencement of CyberSeekAU digital platform optimisation, incorporating forecasting model)	s47(1)(b)	s47(1)(b)	s47(1)(b)

Total Fixed Price for Services **s47(1)(b) GST Inclusive**

Adjustment to Fixed Pricing for Contract Variation/Extension

The initial contract term is for 12 months, with an option for extension. Any rates in the second year would be limited to platform maintenance costs alone, likely to result in a reduction of costs for any future contract and related payment schedule.

C.A.3(a) Payment Schedule

Progress payments of the *Fixed Fees and Charges* (inclusive of any GST and all taxes and charges) will be made as follows:

Estimated Date	Milestone Description	Payment Amount
Early July 2021	Execution of contract and full payment	s47(1)(b)

C.A.4 Contract Managers and Addresses for Notices

Contract Managers are responsible for issuing or accepting any written Notices under this Contract and are the contact points for general liaison.

C.A.4(a) Customer's Contract Manager:

The person occupying the position of:

Currently: s22(1)(a)(ii)

Telephone:

Mobile:

Email Address:

Postal Address: Department of Industry, Science, Energy and Resources
GPO Box 2013
Canberra ACT 2601

C.A.4(b) Customer's Address for Invoices:

Addressee Name/Position Title: s22(1)(a)(ii)

Telephone:

Email Address: cybersecurity@industry.gov.au

Postal Address: Department of Industry, Science, Energy and Resources
GPO Box 2013
Canberra ACT 2601

The Customer's preferred method of invoicing is by email.

C.A.4(c) Supplier's Contract Manager:

Name: s22(1)(a)(ii)

Position Title:

Telephone:

Mobile:

Email Address:

Postal Address: Unit 2, Level 4
1 Hobart Place
Canberra ACT 2600

C.A.4(d) Supplier's Address for Notices

Name: s22(1)(a)(ii)

Position Title:

Email Address:

Postal Address: Unit 2, Level 4
1 Hobart Place
Canberra ACT 2600

C.A.5 Specified Personnel

Position/Role	Name	Current Security Clearance Level	Percentage of Total Project Time
Contact Officer/Project Manager (co-ordination, reporting, preparation of written products)	s22(1)(a)(ii)	N/A	30%
Digital Product Manager (Execution of platform optimisation)	s22(1)(a)(ii)	N/A	40%
Project Support Officer (Research, analysis, workshop facilitation, & project support)	s22(1)(a)(ii)	N/A	30%

C.A.6 Subcontractors

Full Legal Name	Postal Address	ACN / ABN / ACNR	Services to be Performed
Burning Glass Technologies	66 Long Wharf (Floor 2), Boston, MA, 02110, United States	N/A	Only aspects are to be subcontracted that pertain to algorithmic augmentation (to improve timeliness of data reporting and visualisation), as well as related updates to architecture arising from ANZSCO updates in around November 2021. AustCyber will host and maintain the platform, as per current arrangements.

Additional Contract Terms

An executed contract will incorporate the Commonwealth Contract Terms and also the following Additional Contract Terms:

C.B.1 Intellectual Property

The Supplier owns the Intellectual Property Rights in the Material created under this Contract.

The Supplier grants to the Customer:

- a) a non-exclusive, irrevocable, royalty-free, perpetual, world-wide licence to exercise the Intellectual Property Rights in the Material provided under this Contract for any purpose; and
- b) a right to sub-licence the rights in (a) above to third parties, including to the public under an open access or Creative Commons 'BY' licence.

The licence includes the right of commercial exploitation by the Customer.

The Supplier warrants that it is entitled to grant this licence to the Customer; and that the provision of the Goods and/or Services and any Material by the Supplier under this Contract, and its use by the Customer, in accordance with this Contract, will not infringe any third party's Intellectual Property Rights and Moral Rights.

Intellectual Property Rights in Goods provided under this Contract or pre-existing Intellectual Property of the Supplier, set out below (if any), will not change as a result of this Contract.

Pre-Existing Intellectual Property of the Supplier

The Supplier grants to, or in the case of Third-Party Material, must obtain for, the Customer a non-exclusive, irrevocable, royalty-free, perpetual, world-wide licence (including the right to sub-licence) to exercise the Intellectual Property Rights in all Pre-existing Material and Third-Party Material incorporated into the Material to enable the Customer to receive the full benefit of the Goods and/or Services and the Material and to exercise its rights in relation to the Material.

AustCyber will retain ownership of the Intellectual Property Rights in the Material created under the Contract. As the supplier, we will maintain ownership of the model and will retain responsibility for the ongoing maintenance of the model and data.

s47(1)(b)

C.B.3 Interest on Late Payments

Where the Customer and the Supplier both have the capability to deliver and receive e-Invoices through the Pan-European Public Procurement On-Line (PEPPOL) framework and have agreed to use electronic invoicing (e-Invoicing), the Customer will pay the amount of a Correctly Rendered Invoice to the Supplier within five (5) calendar days after receiving it, or if this day is not a business day, on the next business day.

In all other circumstances, the Customer will pay the amount of a Correctly Rendered Invoice to the Supplier within twenty (20) calendar days after receiving it, or if this day is not a business day, on the next business day.

If the total initial value of the Contract (excluding any options, extensions, renewals or other mechanisms that may be executed over the life of the contract) is less than A\$1 million (GST inclusive) and the Customer fails to make a payment to the Supplier by the business day it is due, the Customer will pay the unpaid amount plus interest on the unpaid amount, provided the amount of interest payable under this clause exceeds A\$100.

Interest payable under this clause will be simple interest calculated in respect of each calendar day from the day after the amount was due and payable, up to and including the day that the Customer effects payment, calculated using the General Interest Charge Rate available on the Australian Taxation Office website as it applies on the day the amount was due and payable expressed as a daily rate.

Commonwealth Contract Terms

C.C.1 Background:

The Customer requires the provision of certain Goods and/or Services. The Supplier has fully informed itself on all aspects of the Customer's requirements and has responded representing that it is able to meet the Statement of Requirement.

Some terms used in these *Commonwealth Contract Terms* have been given a special meaning. Their meanings are set out either in the *Commonwealth Contracting Suite Glossary* or in the relevant *Commonwealth Contract*.

C.C.2 Relationship of the Parties:

Neither party is the employee, agent, officer or partner of the other party nor, by virtue of this Contract, authorised to bind or represent the other party.

The Supplier must ensure that its officers, employees, agents or Subcontractors do not represent themselves as being an officer, employee, partner or agent of the Customer.

In all dealings related to the Contract, the parties agree to:

- (a) communicate openly with each other and cooperate in achieving the contractual objectives; and
- (b) act honestly and ethically; and
- (c) comply with reasonable commercial standards of fair conduct; and
- (d) consult, cooperate and coordinate activities to identify and address any overlapping work health and safety responsibilities aimed at ensuring the health and safety of workers and workplaces; and
- (e) comply with all reasonable directions and procedures relating to work health and safety, record keeping and security in operation at each other's premises or facilities whether specifically informed or as might reasonably be inferred from the circumstances.

C.C.3 Conflict of Interest:

The Supplier has either declared any real or perceived conflicts of interest that might arise; or states that no conflicts of interest exist, or are anticipated, relevant to the performance of its obligations under the Contract.

If any conflict or potential conflict arises during the Contract Term, the Supplier will immediately notify the Customer and comply with any reasonable Notice given to the Supplier by the Customer in relation to the conflict. As soon as practicable, any verbal advice must be followed by written confirmation.

C.C.4 Precedence of Documents:

The Contract is comprised of:

- (a) *Additional Contract Terms* (if any);
- (b) *Statement of Work*;
- (c) *Commonwealth Contract Terms*;
- (d) *Commonwealth Contracting Suite Glossary*; and
- (e) *Contract Annex 1 – Supplementary information* (if any),

unless otherwise agreed in writing between the parties.

If there is ambiguity or inconsistency between documents comprising the Contract, the document appearing higher in the list will have precedence.

The Contract may be signed and dated by the parties on separate, but identical, copies. All signed copies constitute one (1) Contract.

C.C.5 Governing Law:

The laws of the Australian Capital Territory apply to the Contract.

C.C.6 Entire Agreement:

The Contract represents the Parties' entire agreement in relation to the subject matter, at the time this Contract was entered.

Anything that occurred before the making of this Contract shall be disregarded (unless incorporated into the Contract in writing). However, the Supplier represents that the claims made in its Response to the ATM were correct when made and remain correct.

The Parties agree that no agreement or understanding varying or extending the Contract will be legally binding upon either Party unless in writing and agreed by both Parties.

If either Party does not exercise (or delays in exercising) any of its contractual rights, that failure or delay will not prejudice those rights.

C.C.7 Survival:

All Additional Contract Terms (if any), plus Clauses C.C.14 [*Liability of the Supplier*], C.C.17 [*Supplier Payments*], C.C.20 [*Transition Out*], C.C.22 [*Compliance with Commonwealth Laws and Policies*], C.C.22(A) [*Access to Supplier's Premises and Records*], C.C.22(F) [*Fraud*] survive termination or expiry of the Contract.

C.C.8 Notices:

A Notice is deemed to be effected:

- (a) if delivered by hand - upon delivery to the relevant address;
- (b) if sent by registered post - upon delivery to the relevant address; or
- (c) if transmitted electronically - upon actual delivery as evidenced by an acknowledgement of receipt from the recipient's system by any means (including by means of delivery receipt).

A Notice received after 5.00 pm, or on a day that is not a working day in the place of receipt, is deemed to be effected on the next working day in that place.

C.C.9 Assignment:

The Supplier may not assign any rights under the Contract without the Customer's written consent. To seek consent, the Supplier must provide the Customer with a Notice, which includes full details of the proposed assignee and the rights the Supplier proposes to assign.

To decline consent, the Customer must provide a Notice to the Supplier, setting out its reasons, within twenty-eight (28) calendar days of receiving the Notice seeking consent. Otherwise, the Customer is taken to have consented.

C.C.10 Subcontracting:

Subcontracting any part of, or the entire Supplier's obligations under the Contract, will not relieve the Supplier from any of its obligations under the Contract.

The Supplier must ensure that Subcontractors specified in Item C.A.6 [*Subcontractors*] (if any) perform that part of the Services Specified in that item. Unless otherwise agreed by the Customer (in writing) the Supplier must not subcontract any part of its obligations under the Contract other than to Subcontractors named in Item C.A.6. The Supplier must ensure that specified Subcontractors (if any) are not replaced without the prior written consent of the Customer. The Customer's written consent will not be unreasonably withheld.

At the Customer's request, the Supplier, at no additional cost to the Customer, must promptly remove from involvement in the Contract any Subcontractor that the Customer reasonably considers should be removed.

Commonwealth Contract Terms

The Supplier must make available to the Customer the details of all Subcontractors engaged to provide the Goods and/or Services under the Contract. The Supplier acknowledges that the Customer may be required to publicly disclose such information.

The Supplier must ensure that any subcontract entered into by the Supplier, for the purpose of fulfilling the Supplier's obligations under the Contract, imposes on the Subcontractor the same obligations that the Supplier has under the Contract (including this requirement in relation to subcontracts).

C.C.11 Delivery and Acceptance:

The Supplier must provide the Goods and/or Services as specified in the *Statement of Work* and meet any requirements and standard specified in the *Statement of Work*.

The Supplier must promptly notify the Customer if the Supplier becomes aware that it will be unable to provide all or part of the Goods and/or Services specified in the *Statement of Work* and advise the Customer when it will be able to so.

Any Goods must be delivered free from any security interest. Unless otherwise stated in the Contract, Goods must be new and unused. Any Services must be provided to the higher of the standard that would be expected of an experienced, professional supplier of similar services and any standard specified in the *Statement of Work*.

The Customer may reject the Goods and/or Services within fourteen (14) calendar days after delivery or such longer period specified in the Contract at Item C.A.2(d) [*Delivery and Acceptance*], if the Goods and/or Services do not comply with the requirements of the Contract ("Acceptance Period").

If during the Acceptance Period circumstances outside the Customer's reasonable control cause a delay in the Customer's evaluation of the compliance of the Goods and/or Services with the Contract, the Customer may give the Supplier a Notice before the end of the original Acceptance Period, setting out the reason for the delay and the revised Acceptance Period date (which must be reasonable having regard to the circumstances causing the delay).

If the Customer does not notify the Supplier of rejection within the Acceptance Period (as extended if applicable), the Customer will be taken to have accepted the Goods and/or Services, though the Customer may accept the Goods and/or Services sooner. Title to Goods transfers to the Customer only on acceptance.

If the Customer rejects the Goods and/or Services, the Customer must issue a Notice clearly stating the reason for rejection and the remedy the Customer requires. No payment will be due for rejected Goods and/or Services until their acceptance.

C.C.12 Licences Approvals and Warranties:

At no cost to the Customer, the Supplier must obtain and maintain all Intellectual Property Rights, licences or other approvals required for the lawful provision of the Goods and/or Services and arrange any necessary customs entry for any Goods.

The Supplier must provide the Customer with all relevant third Party warranties in respect of Goods. If the Supplier is a manufacturer, the Supplier must provide the Customer with all standard manufacturer's warranties in respect of the Goods it has manufactured and supplied.

To the extent permitted by laws and for the benefit of the Customer, the Supplier consents, and must use its best endeavours to ensure that each author of Material consents in writing, to the use by the Customer of the Material, even if the use may otherwise be an infringement of their Intellectual Property Rights and/or Moral Rights.

C.C.13 Specified Personnel:

The Supplier must ensure that the Specified Personnel set out in Item C.A.5 [*Specified Personnel*] (if any) perform the part of the Services specified in that item. The Supplier must ensure that Specified Personnel (if any) are not replaced without the prior written consent of the Customer. The Customer's written consent will not be unreasonably withheld.

At the Customer's reasonable request, the Supplier, at no additional cost to the Customer, must as soon as reasonably practicable replace any Specified Personnel that the Customer reasonably considers:

- (a) is not performing the Supplier's obligations under the Contract to the standard or within the timeframe reasonably required by the Customer;
- (b) is not a fit and proper person; or
- (c) is not suitably qualified to perform the Services.

Any Specified Personnel must be replaced with personnel that are acceptable to the Customer.

C.C.14 Liability of the Supplier:

The Supplier will indemnify the Customer and its officials against any claim, loss or damage arising in connection with any negligent or wilful breach of the Supplier's obligations or representations under the Contract.

The Supplier's obligation to indemnify the Customer and its officials will reduce proportionally to the extent that any act or omission, on the part of the Customer or its officials contributed to the claim, loss or damage.

The Supplier's liability under this clause shall not exceed the maximum applicable amount that applies to the claim loss or damage under a scheme operating under Schedule 4 of the *Civil Law (Wrongs) Act 2002 (ACT)*, or any corresponding State, Territory or Commonwealth legislation, that limits the civil liability of members of particular professions arising from the performance of their professional services, where the Supplier is a member of that scheme, and where that scheme applies to the Goods and/or Services delivered under the Contract.

The Supplier will maintain adequate insurances for the Contract and provide the Customer with proof when reasonably requested.

C.C.15 Termination or Reduction for Convenience:

In addition to any other rights either party has under the Contract,
(a) the Customer acting in good faith, may at any time; or
(b) the Supplier, acting in good faith, may notify that it wishes to, terminate the Contract or reduce the scope or quantity of the Goods and/or Services by providing a Notice to the other Party.

If the Supplier issues a Notice under this clause, the Supplier must comply with any reasonable directions given by the Customer. The Contract will terminate, or the scope will be reduced in accordance with the Notice, when the Supplier has complied with all of those directions.

If the Customer issues a Notice under this clause, the Supplier must stop or reduce work in accordance with the Notice and comply with any reasonable directions given by the Customer.

Commonwealth Contract Terms

In either case, the Supplier must mitigate all loss and expenses in connection with the termination or reduction in scope (including the costs of its compliance with any directions). The Customer will pay the Supplier for Goods and/or Services accepted in accordance with clause C.C.11 [Delivery and Acceptance] and item C.A.2(d) [Delivery and Acceptance] before the effective date of termination or reduction.

If the Customer issues a Notice under this clause, the Customer will also pay the Supplier for any reasonable costs the Supplier incurs that are directly attributable to the termination or reduction, provided the Supplier substantiates these costs to the satisfaction of the Customer.

Under no circumstances will the total of all payments to the Supplier exceed the Contract Price. The Supplier will not be entitled to loss of anticipated profit for any part of the Contract not performed.

C.C.16 Termination for Cause:

The Customer may issue a Notice to immediately terminate or reduce the scope of the Contract if:

- (a) the Supplier does not deliver the Goods and/or Services as specified in the Contract, or notifies the Customer that the Supplier will be unable to deliver the Goods and/or Services as specified in the Contract;
- (b) the Customer rejects the Goods and/or Services in accordance with clause C.C.11 [Delivery and Acceptance] and the Goods and/or Services are not remedied as required by the Notice of rejection;
- (c) the Supplier breaches a material term of the Contract and the breach is not capable of remedy;
- (d) the Supplier does not remediate a material breach of the Contract which is capable of remediation within the period specified by the Customer in a Notice of default issued to the Supplier; or
- (e) subject to the Customer complying with any requirements in the *Corporations Act 2001* (Cth), the Supplier:
 - (i) is unable to pay all its debts when they become due;
 - (ii) if incorporated – has a liquidator, receiver, administrator or other controller appointed or an equivalent appointment is made under legislation other than the *Corporations Act 2001* (Cth); or
 - (iii) if an individual – becomes bankrupt or enters into an arrangement under Part IX or Part X of the *Bankruptcy Act 1966* (Cth).

Termination of the Contract under this clause does not change the Customer's obligation to pay any Correctly Rendered Invoice.

C.C.17 Supplier Payments:

If the Supplier is required to submit an invoice to trigger payment, the invoice must be a Correctly Rendered Invoice.

The Supplier must promptly provide to the Customer such supporting documentation and other evidence reasonably required by the Customer to substantiate performance of the Contract by the Supplier.

Payment of any invoice is payment on account only, and does not substantiate performance of the Contract.

If the Supplier owes any amount to the Customer in connection with the Contract, the Customer may offset that amount, or part of it, against its obligation to pay any Correctly Rendered Invoice.

C.C.18 Dispute Resolution:

For any dispute arising under the Contract both the Supplier and the Customer agree to comply with (a) to (d) of this clause sequentially:

- (a) both Contract Managers will try to settle the dispute by direct negotiation;
- (b) if unresolved, the Contract Manager claiming that there is a dispute will give the other Contract Manager a Notice setting out details of the dispute and proposing a solution;
- (c) if the proposed solution is not accepted by the other Contract Manager within five (5) business days, each Contract Manager will nominate a more senior representative, who has not had prior direct involvement in the dispute. These representatives will try to settle the dispute by direct negotiation;
- (d) failing settlement within a further ten (10) business days, the Customer will, without delay, refer the dispute to an appropriately qualified mediator selected by the Customer or, at the Customer's discretion, to the chairperson of an accredited mediation organisation to appoint a mediator, for mediation to commence within fifteen (15) business days of the request.

Representatives for the Supplier and the Customer must attend the mediation. The nominated representatives must have the authority to bind the relevant party and act in good faith to genuinely attempt to resolve the dispute.

The Customer and the Supplier will each bear their own costs for dispute resolution. The Customer will bear the costs of a mediator.

If the dispute is not resolved within thirty (30) business days after mediation commences, either the Supplier or the Customer may commence legal proceedings.

Despite the existence of a dispute, the Supplier will (unless requested in writing by the Customer not to do so) continue their performance under the Contract.

This procedure for dispute resolution does not apply to action relating to clause C.C.16 [Termination for Cause] or to legal proceedings for urgent interlocutory relief.

C.C.19 Transition In:

The Supplier must perform all tasks reasonably required to facilitate the smooth transition of the provision of the Goods and/or Services from any outgoing supplier to the Supplier.

C.C.20 Transition Out:

If the Contract expires or is terminated under clause C.C.16 [Termination for Cause] the Supplier must comply with any reasonable directions given by the Customer in order to facilitate the smooth transition of the provision of the Goods and/or Services to the Customer or to another supplier nominated by the Customer.

C.C.21 Compliance with Laws:

The Supplier must comply with, and ensure its officers, employees, agents and subcontractors comply with the laws from time to time in force in any jurisdiction in which any part of the Contract is performed.

Commonwealth Contract Terms

C.C.22 Compliance with Commonwealth Laws and Policies:

The Supplier must comply with, and ensure its officers, employees, agents and subcontractors comply with all Commonwealth laws and policies relevant to the Goods and/or Services and must provide such reports and other information regarding compliance as reasonably requested by the Customer or as otherwise required by a relevant law or policy.

If the Supplier becomes aware of any actual or suspected breach of the requirements set out in clauses A to G below, it must:

- (a) immediately report it to the Customer and provide a written report on the matter within five (5) business days; and
- (b) comply with any reasonable directions by the Customer in relation to any investigation or further reporting of the actual or suspected breach.

A. Access to Supplier's Premises and Records: The Supplier must maintain proper business and accounting records relating to the supply of the Goods and/or Services and performance of the Contract.

The Supplier agrees to provide to the Customer, or its nominee, access to the Supplier's, or its Subcontractor's premises, personnel, documents and other records, and all assistance reasonably requested, for any purpose associated with the Contract or any review of the Supplier's or the Customer's performance under the Contract, including (but not limited to) in connection with a request made under the *Freedom of Information Act 1982* (Cth) or audit or review by the Australian National Audit Office. Unless the access is required for the purpose of a criminal investigation into the Supplier, its employees or subcontractors, the Customer will reimburse the Supplier's substantiated reasonable cost for complying with the Customer's request.

The Supplier must not transfer, or permit the transfer of, custody or ownership, or allow the destruction, of any Commonwealth record (as defined in the *Archives Act 1983* (Cth)) without the prior written consent of the Customer. All Commonwealth records, including any held by Subcontractors, must be returned to the Customer at the conclusion of the Contract.

B. Privacy Act 1988 (Cth) Requirements: In providing the Goods and/or Services, the Supplier agrees to comply, and to ensure that its officers, employees, agents and subcontractors comply with the *Privacy Act 1988* (Cth) and not to do anything, which if done by the Customer would breach an Australian Privacy Principle as defined in that Act.

C. Confidential Information: Other than information available in the public domain, the Supplier agrees not to disclose to any person, other than the Customer, any confidential information relating to the Contract or the Goods and/or Services, without prior written approval from the Customer. This obligation will not be breached where the Supplier is required by law 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).

The Customer may at any time require the Supplier to arrange for its employees, agents or subcontractors to give a written undertaking relating to nondisclosure of the Customer's confidential information in a form acceptable to the Customer.

The Customer will keep any information in connection with the Contract confidential to the extent it has agreed in writing to keep such specified information confidential. The Customer will not be in breach of any confidentiality agreement if the Customer is required to disclose the information by law, a Minister or a House or Committee of Parliament.

D. Security and Safety: When accessing any Commonwealth place, area or facility, the Supplier must comply with any security and safety requirements notified to the Supplier by the Customer or of which the Supplier is, or should reasonably be aware. The Supplier must ensure that its officers, employees, agents and subcontractors are aware of, and comply with, such security and safety requirements.

The Supplier must ensure that all information, material and property provided by the Customer for the purposes of the Contract is protected at all times from unauthorised access, use by a third party, misuse, damage and destruction and is returned as directed by the Customer.

The Supplier acknowledges that unauthorised disclosure of security-classified information is an offence. Legislation (including, but not limited to, the *Criminal Code Act 1995* (Cth)) contains provisions relating to the protection of certain information and sets out the penalties for the unauthorised disclosure of that information.

E. Criminal Code: The Supplier acknowledges that the giving of false or misleading information to the Commonwealth is a serious offence under section 137.1 of the schedule to the *Criminal Code Act 1995* (Cth). The Supplier must ensure that any subcontractor engaged in connection with the Contract is aware of the information contained in this clause.

F. Fraud: For the purposes of this clause, Fraud means dishonestly obtaining a benefit from the Commonwealth or causing a loss to the Commonwealth by deception or other means.

The Supplier must take all reasonable steps to prevent and detect Fraud in relation to the performance of this Contract. The Supplier acknowledges the occurrence of Fraud will constitute a breach of this Contract.

If an investigation finds that the Supplier or its employees have committed Fraud, or the Supplier has failed to take reasonable steps to prevent Fraud by an employee or subcontractor, the Supplier must reimburse or compensate the Customer in full.

G. Taxation: The Supplier agrees to comply, and to require its subcontractors to comply, with all applicable laws relating to taxation.



The Commonwealth Contract Terms are licensed under the Creative Commons [Attribution-NonCommercial-NoDerivatives 4.0 International](https://creativecommons.org/licenses/by-nc-nd/4.0/) License (CC BY NC ND 4.0 INT).

Commonwealth Contracting Suite (CCS) Glossary

In the Commonwealth Contracting Suite:

A reference to:

- a) a clause in the form A.A.[x] – is a reference to a clause of the **Approach to Market**;
- b) a clause in the form A.B.[x] – is a reference to a clause of the **Commonwealth ATM Terms**;
- c) an item in the form C.A.[x] – is a reference to an item in the **Statement of Work**;
- d) a clause in the form C.B.[x] – is a reference to a clause in the **Additional Contract Terms**;
- e) a clause in the form C.C.[x] – is a reference to a clause of the **Commonwealth Contract Terms** or the **Commonwealth Purchase Order Terms**, as the case may be.

“Additional Contract Terms” means the terms and conditions set out in the section of the Contract with the heading ‘Additional Contract Terms’.

“Approach to Market or ATM” means the notice inviting potential suppliers to participate in the procurement.

“Closing Time” means the closing time specified in clause A.A.1 [*Key Events and Dates*].

“Contract” means the documentation specified in clause C.C.4 [*Precedence of Documents*].

“Contract Extension Option” means an option of a Customer to extend the term of a Contract for one or more additional time periods.

“Contract Manager” means the contract manager for the Customer and/or Supplier (as relevant) specified in the Contract.

“Contract Price” means the total contract price specified in the Contract, including any GST component payable, but does not include any simple interest payable on late payments.

“Correctly Rendered Invoice” means an invoice that:

- a) is correctly addressed and calculated in accordance with the Contract;
- b) relates only to Goods and/or Services that have been accepted by the Customer in accordance with the Contract;
- c) includes any purchase order number, and the name and phone number of the Customer’s Contract Manager;
- d) is for an amount which, together with all previously Correctly Rendered Invoices, does not exceed the Contract Price; and
- e) is a valid tax invoice in accordance with the GST Act.

“Customer” means a party specified in a Contract as a Customer.

“Delivery and Acceptance” means the process by which Goods and/or Services are delivered to a Customer and accepted by the Customer as meeting the terms specified in the Contract.

“General Interest Charge Rate” means the general interest charge rate determined under section 8AAD of the *Taxation Administration Act 1953* on the day payment is due, expressed as a decimal rate per day.

“Goods and/or Services” means:

- a) the Goods, Services, or Goods and Services and any Material specified in the Contract; and
- b) all such incidental Goods and Services that are reasonably required to achieve the purposes of the Customer as specified in the Contract.

“GST Act” means *A New Tax System (Goods and Services Tax) Act 1999* (Cth).

“GST” means a Commonwealth goods and services tax imposed by the GST Act.

“Intellectual Property Rights” means all intellectual property rights which may subsist in Australia or elsewhere, whether or not they are registered or capable of being registered.

Commonwealth Contracting Suite (CCS) Glossary

“Material” means any material brought into existence as a part of, or for the purpose of producing the Goods and/or Services, and includes but is not limited to documents, equipment, information or data stored by any means.

“Moral Rights” means the rights in *Part IX of the Copyright Act 1968 (Cth)*, including the right of attribution, the right against false attribution and the right of integrity.

“Notice” means an official notice or communication under the Contract in writing, from one Contract Manager and delivered to the other Contract Manager, at the postal address, or email address, or facsimile number set out in the Contract or as notified from time to time.

“Requirement” means the description of the Goods and Services described in:

- a) for the purposes of the Commonwealth ATM Terms the section of the Approach to Market with the heading ‘Requirement’;
- b) for the purposes of the Commonwealth Contract Terms the section of the Statement of Work with the heading ‘Requirement’;
- c) for the purposes of the Commonwealth Purchase Order Terms the document setting out the Goods and/or Services.

“Specified Personnel” means the personnel specified in the Contract or such other personnel who are accepted by the Customer in accordance with clause C.C.13 [*Specified Personnel*].

“Statement of Requirement” means the section of the Approach to Market with the heading ‘Statement of Requirement’.

“Statement of Work” means the section of the Contract, as the case may be, with the heading ‘Statement of Work’.

“Supplier” means a party specified in a Contract as a Supplier.

Contract Signing Page

The Parties agree that by signing this Commonwealth Contract – Services, they enter into a Contract comprising:

- a) Additional Contract Terms (if any);
- b) Statement of Work;
- c) Commonwealth Contract Terms;
- d) Commonwealth Contracting Suite Glossary; and
- e) Contract Annex 1 – Supplementary Information (if any).

EXECUTED as an Agreement

Signed for and on behalf of the **Commonwealth of Australia** as represented by Department of Industry, Science, Energy and Resources

ABN 74 599 608 295 by its duly authorised delegate in the presence of

Signature of witness

Signature of delegate

Name of witness (**print**)

Name of delegate (**print**)

Position of delegate (**print**)

Date:

Executed by AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED **ABN** 73 616 231 451 in accordance with Section 127 of the *Corporations Act 2001*

Signature of director

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

Name of director (**print**)

Name of director/company secretary (**print**)

Date:



Workforce Skills

DRAFT
PROJECT MANAGEMENT PLAN

Prepared July 2021

TABLE OF CONTENTS

1. PROJECT OVERVIEW, 3
2. PROJECT TIMELINES, 8
3. RISK MANAGEMENT, 12
4. BUDGET, 14
5. LAUNCH, 15
6. PROJECT TEAM, 16

PROJECT OVERVIEW

SUMMARY

This project is an initiative under the Australian Government's *Cyber Security National Workforce Growth Program*. This Program is designed to develop the cyber security skills required now, while creating a pipeline of skilled Australians going forward.

PROJECT REQUIREMENTS

The Department of Industry, Science, Energy and Resources (the Customer) has sought expertise to **develop or expand a forecasting methodology and model for analysing the Australian cyber security workforce and skills** shortages in real-time and to provide regular data reporting to the Customer.

This solution would be publically available to enable industry, education, government and the broader Australian community to access this information. The project aims to strengthen cyber security skills forecasting, labour force and workforce demand data to better understand the current environment and inform future government policies.

The data underpinning this work will feed into, or draw from, other agencies' (for example, the Australian Bureau of Statistics; or National Skills Commission; or Department of Education, Skills and Employment) data initiatives and sources as much as possible to minimise duplication and embed long term solutions to data gaps.

PROJECT ON A PAGE



- Table of Contents Summary report.
- Detailed written summary report outlining Australia's current CS workforce skills and capabilities.
- A workshop to support Supplier and Customer collaboration to shape inputs, definitions and the forecasting model codesigned with DISER.

- Improve and develop the existing Cyber Seek product or to develop a new modelling tool, to provide forecasting data on CS workforce and skills including oversupply, shortages and to provide insights into international comparisons.

- Once the modelling tool is developed both parties will continue to collaborate on specific data outputs.
- CS will continue to update the modelling tool and any associated reporting tools.

Product: We can significantly augment and improve our existing platform, CyberSeek in response to the requirement to “develop a new model, or configure an existing model to deliver the project requirements.

Reporting: An agreed report template will be developed for routine (quarterly) provision of data to the Customer

STAGE 1

The **first stage** of the project will include a **comprehensive outline and a detailed written summary report** which will outline the current state of Australia's cyber security workforce and skills and capabilities. The report will include detailed information on data points and sources available for emerging areas of interest in workforce skills and shortages in Australia and internationally.

The report will map out the current number of Australians employed in the cyber security workforce as well as existing advertised job vacancies.

The report will summarise the most common cyber security qualifications in the Australian labour market, it will include a detailed glossary of terms. And an appendix of all data sources

Report information will leverage the NICE framework to frame occupations and job roles and enable international comparison of performance. In conducting this analysis, an inclusion of a comparative overview for the United States, United Kingdom, New Zealand, and Germany; countries where baseline data exists will occur, enabling some comparisons to be made (for example, in areas such as met, oversupply, or shortage.

Finally, we will **co-design a workshop** to be convened to support Supplier and Customer collaboration to shape inputs, definitions and subsequent forecasting model.

STAGE 2

In order to deliver the model and forecasting data required the project will utilise and improve its existing platform, CyberSeek to provide forecasting data on the cyber security workforce and skills and capability supply, including oversupply and shortages allowing the Customer and broader stakeholders to better understand Australia's position and how it compares internationally.

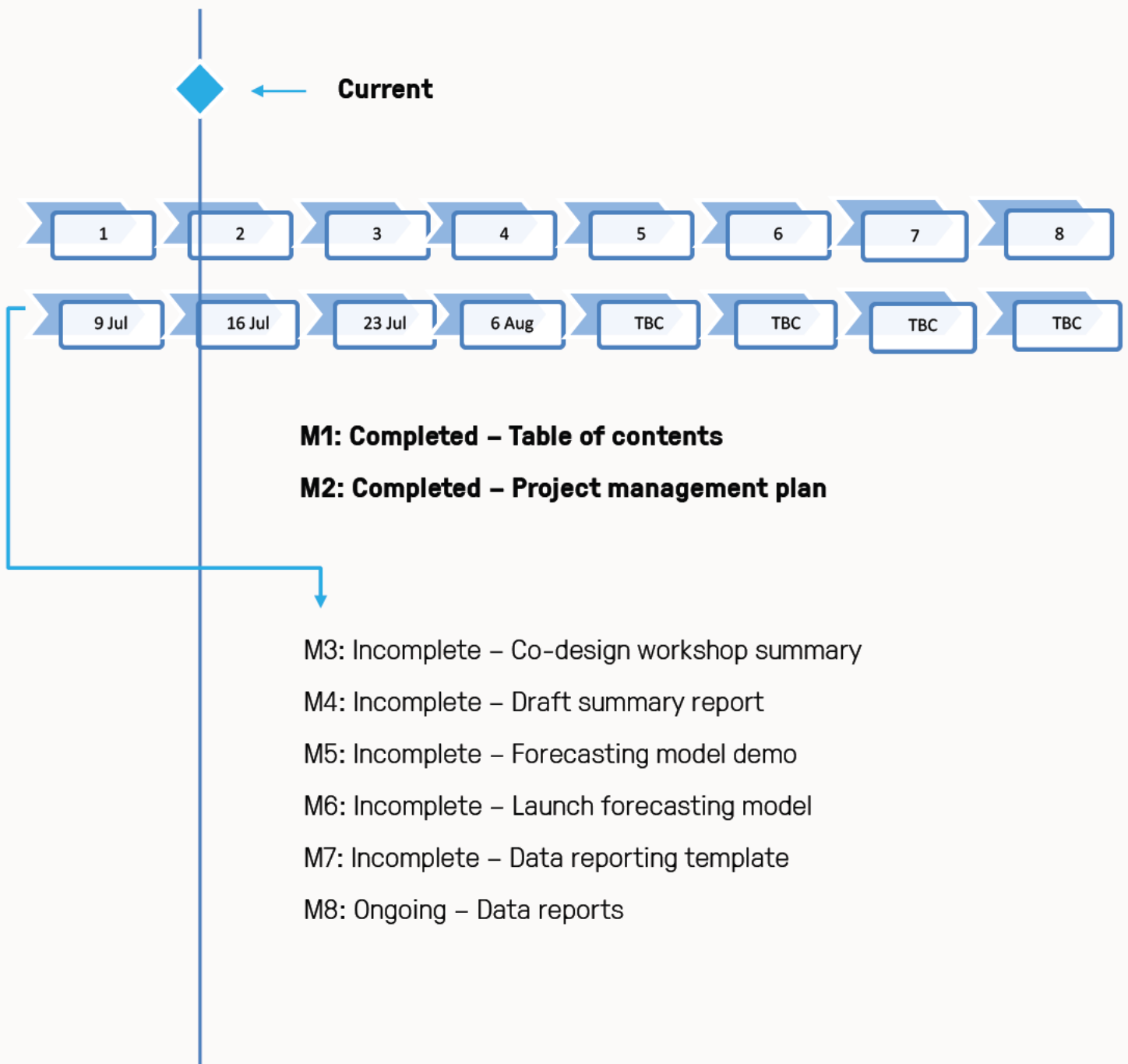
The Customer and Supplier will continue to collaborate on specific data outputs and availability of these throughout the course of the contract term which may include baseline data of the Australian workforce, the Cyber Security workforce recruitment and cyber security training and education offerings.

The project will deliver a **cyber security workforce and skills forecast** and a summary of information on factors impacting the workforce and skills forecasts.

At the completion of the project we will continue to own and maintain the product including **ongoing modelling and forecasting of which all outputs will be made publicly available.**

TIMELINE

KEY MILESTONES



MILSTONE OVERVIEW

The contracted timeline spans a 12month period with a potential option to extend the project for a further 12 month period. The first 4 milestones across the project timeline have confirmed set deliverable dates.

M1	M2	M3	M4
Comprehensive outline (as a Table of Contents) of the proposed summary report on the state of cyber security workforce and skills shortages in Australia delivered	Draft project management plan and proposed project plan delivered	Co-design workshop – summary report	Draft summary report delivered

The second 4 milestones across the project timeline have tentative set deliverable dates to be mutually agreed between the project team and the customer.

M5	M6	M7	M8
Forecasting Model demonstration involving the department (and may involve other relevant stakeholders with a vested interest in cyber security workforce and skills forecasting)	Launch of Forecasting Model	Launch of Forecasting Model	Ongoing Cyber Security Data Reports at an agreed frequency

RISK

AND MITIGATION STRATEGIES

Throughout the life of the project we will **maintain a RAID (Risk, Assumptions, Issues, Dependencies) register**. The RAID will be maintained to ensure that risks are appropriately identified and mitigated ongoing.

Any risks identified will be reported to the project owner on a weekly basis, and will also be included and maintained in the project steering committee meetings and client meetings including the monthly and quarterly updates. Below is an extract from the **initial version of the register**.

⌵ Na...	📝 Notes	⌵ Description + Mitigation	📅 Date Opened	📅 Date Closed	📊 Status Likelihood	📊 Impact
Risk 1	Inability to engage industry/employer partners	To manage the risk of relying on external vendors/sub contractor used when selecting any third-party supplier. For this project we have only engaged with one party at this time who is an existing vendor of the Cyber Seek Product and delivery. We have ensured appropriate contingencies are built into ...	7/12/2021		High	High
⚡ Risk 2	Key resources leave the project	To ensure the movement of key team members does not impact the project delivery the project team and workstream lead will ensure x2 resources are across the workstream lead, deliverables, timeline and accountabilities.	7/12/2021		Low	High
Risk 3	Inability to obtain data and information	The Product Manager and IT Teams to will ensure we have the infrastructure, resources and ,means to deliver of the product and data requirements that Aust Cyber are contractually bound to deliver.	7/12/2021		Medium	High
Risk 4	Financial and/or budget not managed or tracked appropriately	Product and IT Team to manage, track and maintain all vendor costs and expenses related to the project to ensure budgets are maintained throughout the life of the project and our contractual obligations.	7/12/2021		Low	High

BUDGET

Fee for Service Overview (allocations per deliverable):

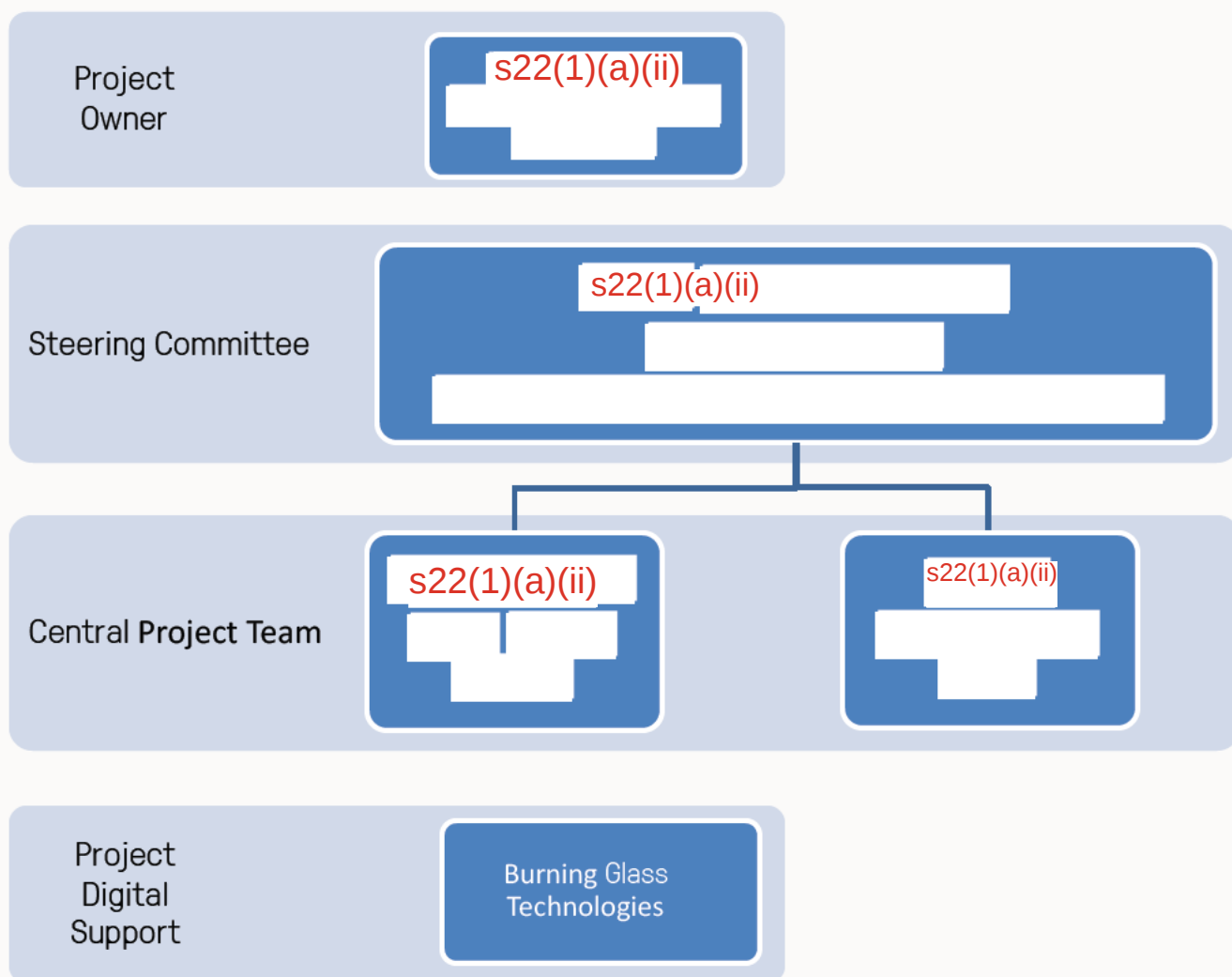
Description	Allocation	Total excl. GST	GST	Total incl. GST
Deliverable One: (Including outline, project plan and written summary report)		s47(1)(b)	s47(1)(b)	s47(1)(b)
Commencement of CyberSeekAU digital platform optimisation, incorporating forecasting model		s47(1)(b)	s47(1)(b)	s47(1)(b)
			Total:	s47(1)(b)

LAUNCH

The new forecasting model and report will be released in a manner agreed between the supplier and the customer at a date to be mutually agreed.

PROJECT TEAM

To deliver this project a **cross-functional project team** have been stood up across AustCyber. The program is leveraging a workstream structure to deliver the multiple deliverables concurrently, with additional support from across AustCyber, as required.



WORKSTREAM LEADS

Team Member	Workstream
s22(1)(a)(ii)	Contact Officer/Project Manager (co-ordination, reporting, preparation of written products)
s22(1)(a)(ii)	Contact Officer/Project Manager (co-ordination, reporting, preparation of written products)
s22(1)(a)(ii)	Project Support Officer (Research, analysis, workshop facilitation, & project support)
s22(1)(a)(ii)	IT Support and lead (overarching IT infrastructure support)
s22(1)(a)(ii)	Head of Communications, Events & Marketing (communications support)

MEETINGS & RHYTHM

Meeting Type	Position Required	Frequency
Initial Project Scoping Meeting	supplier CEO and relevant project management staff	One-Off
Progress Meetings	Relevant project management staff	Monthly
Relevant project management staff	Relevant project management staff	One-Off
End of Project Meeting	Supplier CEO and relevant project management and technical staff as needed	One-Off
Steering Committee Meetings	Relevant project management staff	Bi Monthly
Project Team/Workstream Meeting	Relevant project management staff	Weekly

www.stoneandchalk.com.au

www.austcyber.com

DISER/AustCyber - Milestone 3: Co-design Workshop

Via Cisco Webex (invitation distributed through email)

Date: Tuesday Aug 24, 2021 3pm – 4pm

Attendees:

AustCyber: s22(1)(a)(ii)

DISER: s22(1)(a)(ii), Cyber Security Policy Team

	Item	Lead
1	Quick Summary & Update (including overview of data pull)	s22(1)(a)(ii)
2	Discuss Forecast Inputs & Definitions Prepared questions (refer to below)	s22(1)(a)(ii)
3	Other Agreed Outcomes and Next Steps: a. Agree on date for final amendments to Draft Report b. Agree on the delivery timeline for Milestones 5-7 (including contingencies) c. Agree on high level revisions to risk management matrix	s22(1)(a)(ii)

Please consult:

- ***ATTACHED: Slide Deck***
- ***BELOW: Questions for discussion***

Prepared Questions for Discussion:

Data needs

1. What are the primary drivers of the need for data from a policy, or broader stakeholder, perspective?

Data structure for public consumption

2. In addition to the existing fields on AUCyberExplorer (i.e. State/Territory, NICE Category), what are other fields that can be added to optimise the site?
3. Is the existing geographic visualisation of advertised vacancies adequate (i.e. metro areas and beyond)?
4. How often should data, through algorithmic changes, be updated on the public facing site (i.e. at what intervals - monthly, quarterly, six monthly?)
5. Should the site enable visual comparisons in labour market mobility (i.e. month by month, or quarter-by-quarter, annually, or otherwise?)

Data formatting for reporting

6. What data format is preferred for the Department and other stakeholders (i.e. .csv etc.?)
7. Is the current data pull request form comprehensive enough to meet likely future Departmental needs?

Cyber Skills Project

*Co-design workshop with the Department of Industry, Science,
Energy and Resources (DISER)*

August 2021

AGENDA

- 1. Summary and update
- 2. Forecast inputs & definitions (inclu. prepared questions)
- 3. Other agreed outcomes and next steps

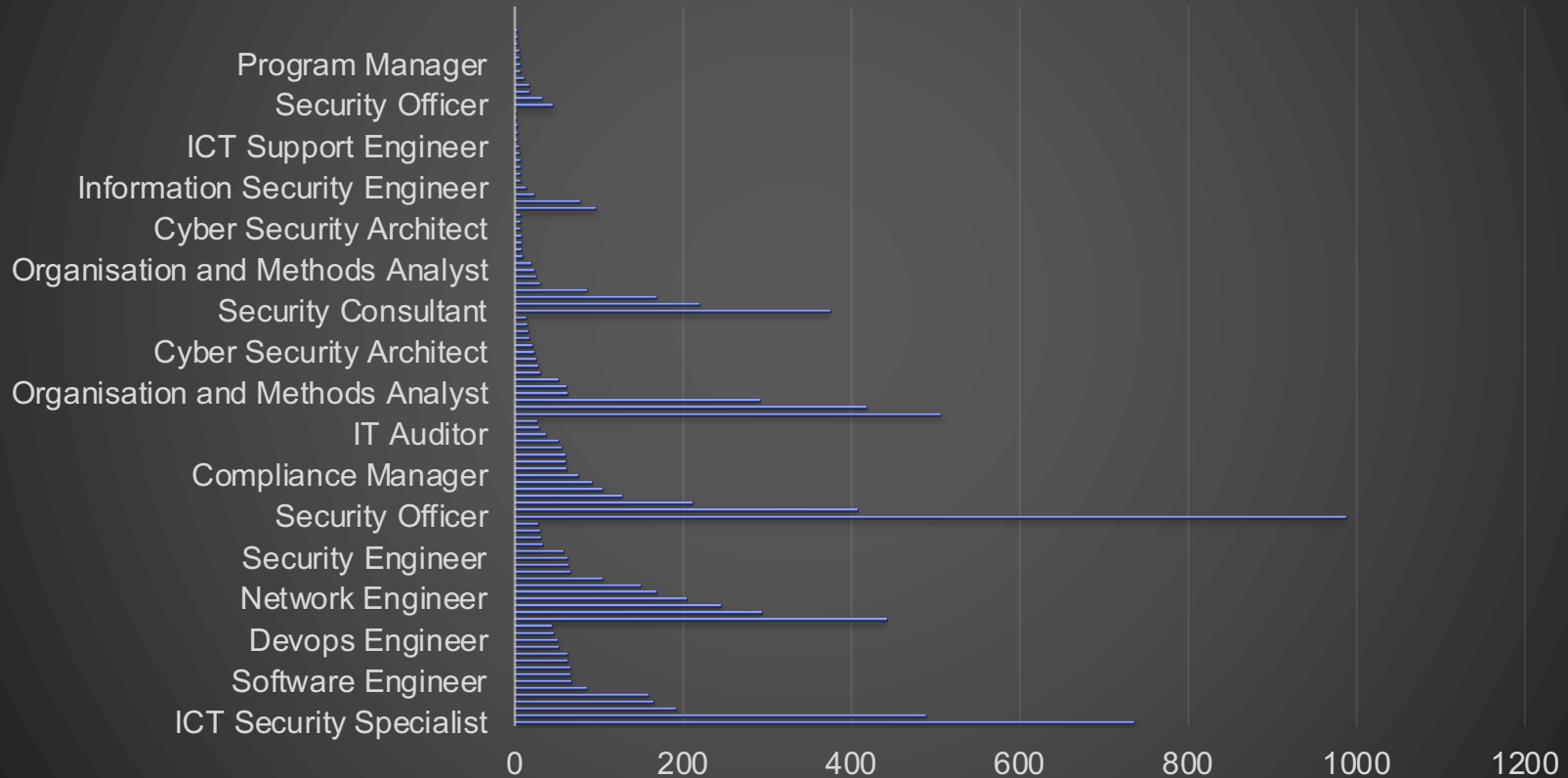
1. SUMMARY AND UPDATE

The background of the slide is a blue gradient, transitioning from a darker blue at the top to a lighter blue at the bottom. Overlaid on this gradient is a complex network of white lines and dots, forming a series of interconnected triangles and polygons. These geometric shapes are scattered across the slide, with some being more prominent than others. The overall effect is a modern, tech-oriented aesthetic.

//

For 'ICT Professionals' (ANZSCO 2 Digit level), there were approx. 300,00 workers (83% of which were male), who held over 410,000 qualifications."

Standardized Job Title Postings in Australia – NICE framework



2. FORECAST INPUTS & DEFINITION

The background of the slide is a blue gradient, transitioning from a darker blue at the top to a lighter blue at the bottom. Overlaid on this gradient are several white geometric shapes, primarily triangles and polygons, connected by thin white lines. These shapes are scattered across the slide, with a more complex cluster of interconnected lines and dots on the right side, resembling a network or a molecular structure. The overall aesthetic is modern and technical.

PHASE TWO

AUCyberExplorer –
optimising the site and
providing new
features (fields,
integration and
accessibility)



PROJECT COLLABORATION MODEL

Key Partners  DISER Burning Glass CompTIA	Key Activities  DISER-AC Workshop Back-end integration with partners Final review of changes w. DISER Full website re-design and optimisation (October/Nov 2021)	Communications plan  Optimised website launch Contact points for data pull requests (for DISER, as Government co-ordination point)
	Key Resources  Reporting template (data pull) Final report Data sources	

STEP WISE PROCESS...

AUCyberExplorer Optimisation

Integration work (within AustCyber)

Agreement with DISER on changes (including new fields)

2

Stocktake

Delivery of summary report to DISER

1

Co-design workshop (technical focus)

Live launch

Activation of refreshed website, public launch

3

Accommodation of ANZSCO changes

CURRENT DATA FIELDS

Field description		Job Role	Category classification	Explanatory Notes
1	NICE framework	×	✓	■ All advertised roles are classified, and aggregated, according to the NICE categories ■ Data is not further disaggregated (i.e. by job role)
2	Location	×	✓	■ Data can be disaggregated by State/Territory/National, and further by metro/non-metro area ■ However, data is not updated in real-time

DATA FIELDS FOR CONSIDERATION...

NICE Category

Data should be categorized according to the NICE Framework

ANZSCO code

Data should be categorized according to the revised ANZSCO codes

Location

Data should be discoverable by each and every Australian State and Territory, as well as Nationally

NICE job role

Data should be discoverable by standardised job role

Gender

Wherever possible, data should be disaggregated by gender (Male/Female/X,) as consistent with the provisions of the *Sex Discrimination Act (1984)*

WHAT INDICATORS HAVE WE MISSED?

APPLICABILITY

Are they needed?

A

F

FIT-FOR-PURPOSE

Do they provide what users are seeking (granularity, proximity to what is being measured etc.)?

E

D

Are they independently powerful or proxies vis-a-vis other indicators?

EXPLANATORY POWER

Is there another public source of data that aligns?

DUPLICATION



3. OTHER AGREED OUTCOMES AND NEXT STEPS

DRAFT ROADMAP

AUGUST 2021:
Co-design workshop

1

SEPTEMBER 2021:
AustCyber internal summary
of technical requirements

3

NOVEMBER 2021:
Final written agreement on
optimisation features w. DISER

5

AUGUST 2021:
Summary of feedback/
finalisation and improvement of
draft report (delivery to DISER)

2

OCTOBER 2021
Presentation to DISER on
proposed draft enhancements
to AUCyberExplorer

4

NOVEMBER 2021:
Execution of changes,
refreshed website goes
live

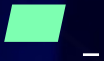
6

A person is wearing a VR headset, looking upwards. The image is overlaid with a blue tint and a white network diagram consisting of interconnected nodes and lines. The text 'THANK YOU' is prominently displayed in the upper left.

THANK YOU

Any questions?

Welcome further written feedback:





WORKING DRAFT: CYBER SKILLS FOR A DIGITAL ECONOMY: AN AUSTRALIAN PROFILE

CYBER SECURITY WORKFORCE AND SKILLS
SHORTAGES IN AUSTRALIA

AUTHORS

Suggested citation: AustCyber (2021). *Cyber Skills and Jobs for a Digital Economy: An Australian Profile. A report for the Department of Industry, Science, Energy & Resources.* Canberra: AustCyber.

To the extent permitted by law, all rights are reserved and no part of this publication covered by copyright may be reproduced or copied in any form or by any means except with the written permission of © AustCyber 2021.

CONTENTS

	Page
ABOUT AUSTCYBER.....	2
REPORT BACKGROUND.....	5
SCOPE OF THE REPORT.....	6
METHODOLOGY.....	7
EMPLOYMENT & SKILLS FOOTPRINT.....	11
CONCLUSION/REPORT SUMMARY.....	
1. Appendix One: Summary Data Sources	
2. Appendix Two: Data Reporting Request Template	
3. Appendix Three: Australian CyberExplorer Optimisation	
4. Appendix Four: Glossary Of Terms	





ABOUT US

AustCyber was established in 2017 as an independent, not-for-profit organisation. We are funded by federal government grants and form a part of two national programs:

- We are part of the federal government's Industry Growth Centres Initiative which was established through the National Innovation and Science Agenda. AustCyber is one of six centres that have been set up in sectors of competitive strength and strategic priority to boost innovation and science in Australia.
- We are an important part of Australia's Cyber Security Strategy as a key enabler for cyber security research and development, as well as innovation.

Our program of activities is underpinned by evidence gained through extensive research and consultation. Our flagship Sector Competitiveness Plan, updated as recently as 2020, outlines the opportunity for Australia's cyber security sector to support growth across the whole economy. We are guided by our Board of esteemed members who have significant industry experience. Our team come from a variety of backgrounds including academia, government and industry.

BACKGROUND

This report is designed to outline the current state of Australia's cyber security workforce and skills and capabilities. The report includes detailed information on data points and sources available for emerging areas of interest in workforce skills and shortages in Australia and internationally.

The report includes a detailed National overview of the current number of Australians employed in the cyber security workforce as well as existing advertised job vacancies.

This report provides a detailed overview and summary of the most common cyber security qualifications in the Australian labour market.

Report information will leverage the NICE framework to frame occupations and job roles and enable international comparison of performance. In conducting this analysis, an inclusion of a comparative overview for the United States, United Kingdom, New Zealand, and Germany; countries where baseline data exists will occur, enabling some comparisons to be made (for example, in areas such as met, oversupply, or shortage).



SCOPE

This report adopts a mixed methods approach to be able to catalogue, describe and analyse available data sources relating to cyber security skills and qualifications in the Australian market. It synthesizes data from a range of sources, to provide an evidence base to inform the optimization of what has been known as CyberSeek AU. This optimization process will be driven by a step-wise approach, underpinned by this report.

These sources include:

- CyberSeek disaggregated data, mapped according to the NICE framework and according to specific roles (sought from a data eco-system partner)
- Public and commissioned reports (including the *Cyber Security Sector Competitiveness Plan 2020*, and the *AustCyber Digital Census 2020*)
- ABS, NSC and NCVER data (where categorization, seasonally, is at a higher, aggregated level)

Data was included if it met one, or a number, of the following criteria:

- pertained to current cyber security job vacancies within Australia
- projected future labour market variation in relation to cyber security within Australia
- outlined methodological challenges to data collection relating to cyber security and the labour market in Australia

Consistent with the data collection and classification protocol adopted by Cyberseek, this report leverages the NICE framework. Developed by the United States National Institute for Standards and Technology (NIST), the NICE Framework has been adopted globally, for the breadth and depth of coverage it provides for the cyber security industry, and it reflects also specific job roles.

In the absence of real-time, and more granular, ABS data, this report uses existing vacancies, as recorded through CyberSeek AU, as a proxy to determine changes (at least in terms of current demand) in the Australian cyber security workforce. This data pertains to live job advertisements, accompanied by detailed role descriptions, for companies domiciled, or with a significant employment footprint, in Australia.

METHODOLOGY

This report adopts a mixed methods approach to be able to catalogue, describe and analyse available data sources relating to cyber security skills and qualifications in the Australian market. The overarching question was: what systems of classification exist in Australia for cyber security roles and the secondary question was: how many cyber security roles exist in Australia and who fills these roles.

Data was scraped from Au CyberSeek, formally sought through a pull request (from all channels that are aggregated to the CyberSeek dashboard, and grey literature was obtained from within the repository of AustCyber.

Cyber security has traditionally been understood in terms of hardware, software and services. The diversity and sophistication of modern cyber security means that this categorisation is no longer appropriate. The way in which we classify skills in Australia, including in relation to cyber security, has long been contested. In some cases, including for migration skills lists, definitions have been inadequate, with only generic ICT categories in operation within ANZSCO, for example. This challenge is not unique, although other countries have more readily adopted frameworks to address this gap in the taxonomy of skills and job roles within cyber security. A range of international definitions and systems of classification have been adopted, for example, emanating from the United Kingdom (i.e. CyBOK) and the United States (NICE Framework). Some of these have been adopted within Government frameworks, and others have been leveraged by industry, to develop tools to map data more effectively and accurately.

Different classification systems for occupations – CyBOK, NICE, ANZIC, ANZSCO

Below we describe the different taxonomies for classifying cyber security skills and qualifications.

The **Cyber Security Body of Knowledge (CyBOK)** is an international collaboration headed by the University of Bristol that structures cyber security according to five main categories:

- **Infrastructure security:** securing computer and digital networks and related physical hardware and systems from intruders and intrusions, whether targeted or opportunistic.
- **Systems security:** operational, network and systems security that includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
- **Software and platform security:** security that focuses on keeping software and an entire computing platform and devices – including mobile, cloud and web applications – resilient to cyber threats. This includes information security that protects the integrity and privacy of data, both in transit and at rest.

- **Attacks and defences:** a proactive and adversarial 'attack' approach to protecting against cyber attacks, which includes penetration and vulnerability testing as well as ethical hacking. Defensive security focuses on reactive measures such as patching software and detection.
- **Human, organisational and regulatory aspects:** tools and services to protect against intentional and unintentional user mistakes; support observance of organisational governance and policies; and enforce compliance with regulatory requirements.

The NICE Framework

The National Initiative for Cybersecurity Education (NICE) have established a [workforce framework](#) that establishes a taxonomy and common lexicon that describes cyber security work and workers irrespective of where or for whom the work is performed.

The NICE Framework is intended to be applied in the public, private, and academic sectors.

It is comprised of the following components:

- Categories (7): A high-level grouping of common cyber security functions.
- Specialty Areas (33): Distinct areas of cyber security work.
- Work Roles (52): The most detailed groupings of cyber security work. This includes specific knowledge, skills, and abilities required to perform tasks in a work role.

The NICE Framework can be harmonised with official Government frameworks, as it provides both a granular (role-centric), as well as an aggregate view of the broad spectrum of cyber related roles. Due to its adoption in the US Market, and benchmarking elsewhere, it also provides a robust framework for comparative analysis between different labour markets.

Framework	Provides broad classification for the cyber security field	Provides specific sub-categorization for cyber roles	Adopted widely outside of originating country(s)
ANZSCO	YES		
CyBOK	YES	YES	YES
NICE	YES	YES	YES

EMPLOYMENT AND SKILLS FOOTPRINT

(NB – This is being populated by a data pull
– week of 16/08/21, which maps all job
roles across Australia)

Attachment A

Cyber Security Occupations – For Cyberseek data request

Cyber security functional roles	Identified roles (ASD ¹ Cyber Security Skills Framework*)	Identified roles from stakeholder submissions	Identified roles from Cyberseek	Identified roles from the NICE Framework	# Existing vacancies for Sydney and Melbourne Metro areas (July 2021) – by NICE Category
Cyber Security Analysis	1. Cyber Threat Analyst*	Information Security Governance, Risk & Compliance (Auditor, Analyst, Implementor or Manager roles)	Cyber Security Analyst	Threat/Warning Analyst	Analyze Sydney • 339 Melbourne • 166
	2. Intrusion Analyst*		Cyber Crime Analyst / Investigator	Target Network Analyst	Analyze Sydney • 339 Melbourne • 166
	3. Malware Analyst*			Cyber Forensics Analyst	Protect & Defend Sydney • 923 Melbourne • 570

¹ ASD Cyber Skills Framework – Cyber Security Occupations
<https://www.cyber.gov.au/sites/default/files/2020-09/ASD-Cyber-Skills-Framework-v2.pdf>

Cyber Security Operations	4. Incident Responder*		Incident Analyst /Responder	Cyber Defence Incident Responder	Protect & Defend Sydney • 923 Melbourne • 570
	5. Operations Coordinator*	Security Project/Program Manager	Cyber Security Manager /Administrator	Cyber Operations Planner	Collect & Operate Sydney • 356 Melbourne • 172
Cyber Security Testing	6. Penetration Tester*	Application Security Consultant / Secure Software Developer	Penetration and Vulnerability Tester	Cyber Defence Analyst	Protect & Defend Sydney • 923 Melbourne • 570
	7. Vulnerability Assessor*		IT Auditor	Vulnerability Assessment Analyst	Protect & Defend Sydney • 923 Melbourne • 570
Cyber Security Architecture	8. Cyber Security Advice and Assessment*		Cyber Security Consultant / Cyber Security Specialist	Cyber Defence Analyst	Protect & Defend Sydney • 923 Melbourne • 570

	9. Vulnerability Researcher*	Security Architect	Cyber Security Architect /Cyber Security Engineer	<i>Research and Development Specialist</i>	Securely provision Sydney • 2133 Melbourne • 1302
--	------------------------------	--------------------	---	--	--

Cyber Security non-technical roles					
Cyber Security Functional Roles	Specific roles identified	Specific responsibilities	Related occupation titles		
Training, Education and Awareness.* ²	10. Security Training, Awareness and Communication	Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers and/or evaluates training courses, methods, and techniques as appropriate.	- Cyber Instructional Curriculum Developer - Cyber Instructor	Training, Education & Awareness	Oversee & Govern Sydney • 1466 Melbourne • 821
Legal Advice and Advocacy*	11. Cyber Legal Advisor	Provides legal advice and recommendations on relevant topics related to cyber law.	Cyber Legal Advisor	Legal Advice & Advocacy	Oversee & Govern Sydney • 1466 Melbourne • 821
	12. Privacy Officer/Privacy Compliance Manager	Develops and oversees privacy compliance program and privacy	Cyber Privacy Officer/	Legal Advice & Advocacy	Oversee & Govern Sydney

² These are NICE framework cyber security functional domains.

		program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams.			• 1466 Melbourne • 821
--	--	--	--	--	--

COMMON QUALIFICATIONS (AUSTRALIAN MARKET)

Overview:

- Australia is a qualified and credentialed country, although not all training in the ICT area is accredited
- In 2018-19 alone, an estimated 10.2 million people reported holding 15.4 million qualifications
- VET qualifications, at a population level, are more common, particularly at CERT III/IV Levels
- Available data for 'ICT Professionals,' which currently subsumes cyber security related roles (at the ANZSCO 2-digit level), shows that **out of a total of 300,000 workers (83% male), they held over 410,000 qualifications.**
 - 52.7% held a single qualification
 - 37.6% held two or more qualifications

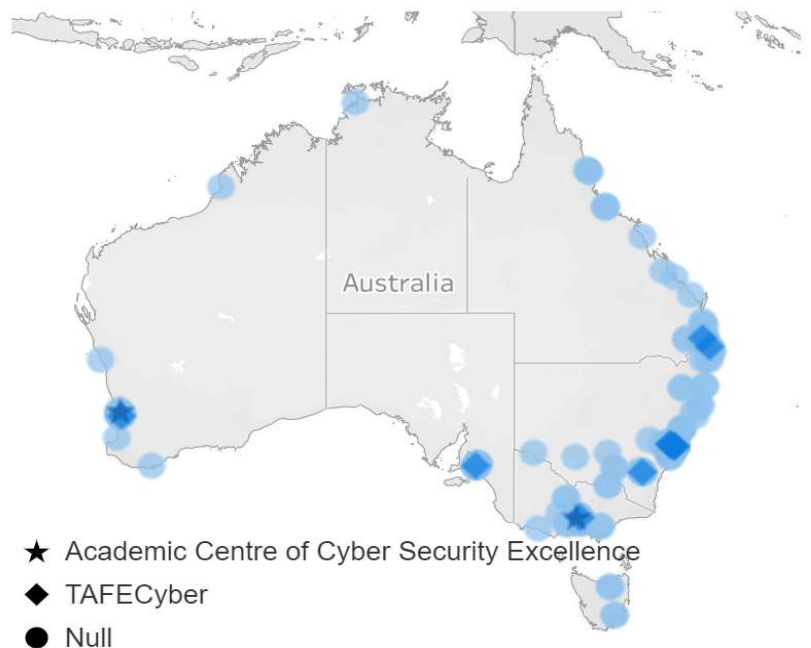
- *Source: Hall & Stanwick (2021).*

AUSTRALIAN CYBER SECURITY : TERTIARY QUALIFICATIONS

Australian tertiary providers offer a wide range of qualifications, incorporating specific cyber security courses.

The Eastern Seaboard States, including NSW, Queensland and the ACT, as well as Victoria, offer the highest number in aggregate.

We have provided a breakdown, by State and Territory, of the number of cyber courses offered across Australia, stratified by State and Territory.



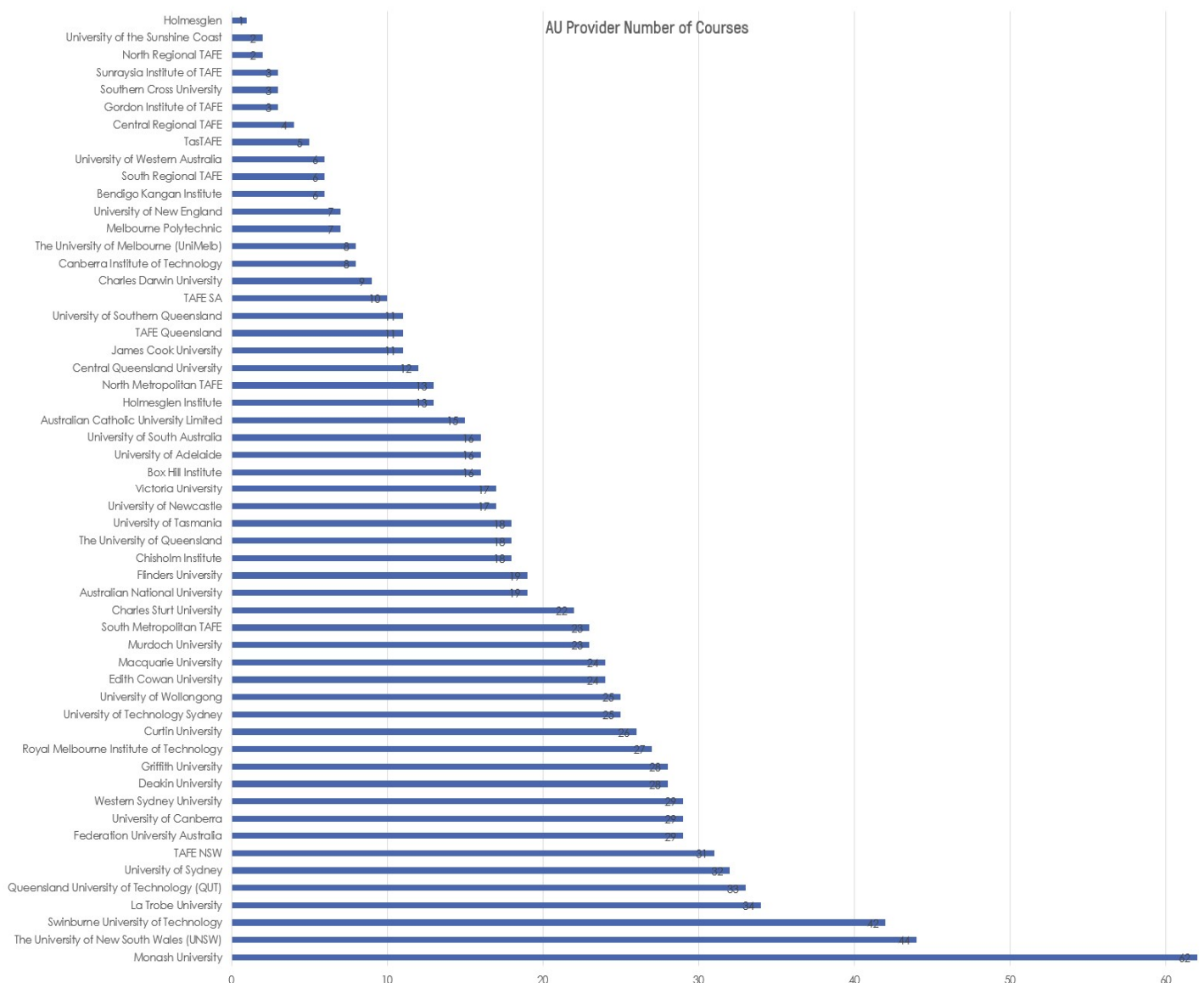
Courses By State



National Courses By Institution

Unsurprisingly, there is a clustering and concentration of cyber security courses, stratified by institution, in both NSW and Victoria.

Each of the top ten highest course providers (by number of qualifications), are from either State. The number of advertised and listed offerings varies greatly, by institution type, with Universities, according to this data, offering a greater variety and number of qualifications, through to Doctoral level study.



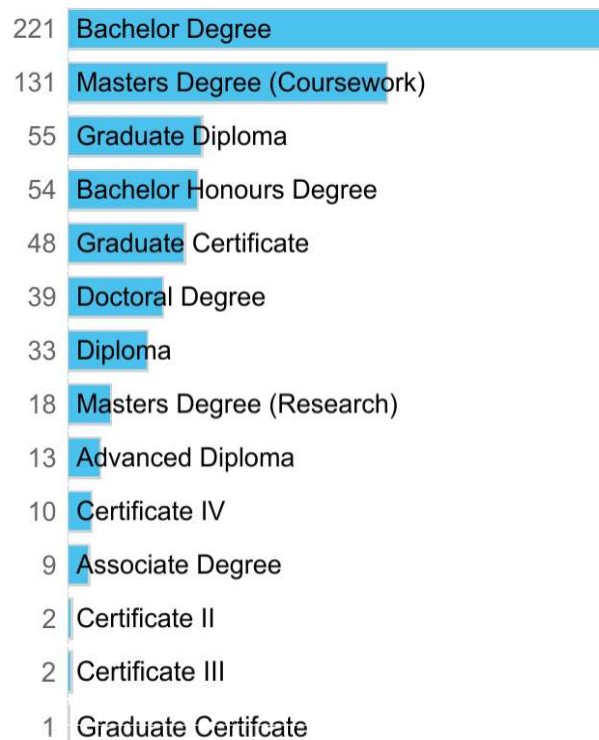
National Courses: By Qualification Level

The Australian cyber security educational landscape is served by a high number of undergraduate qualifications, primarily through bachelor degrees, diplomas and certificates.

There are notable offerings at Masters and Doctoral level too, and an array at graduate level, ranging from Graduate Certificates to Masters (by coursework and research), and Doctoral, degrees.

Course duration

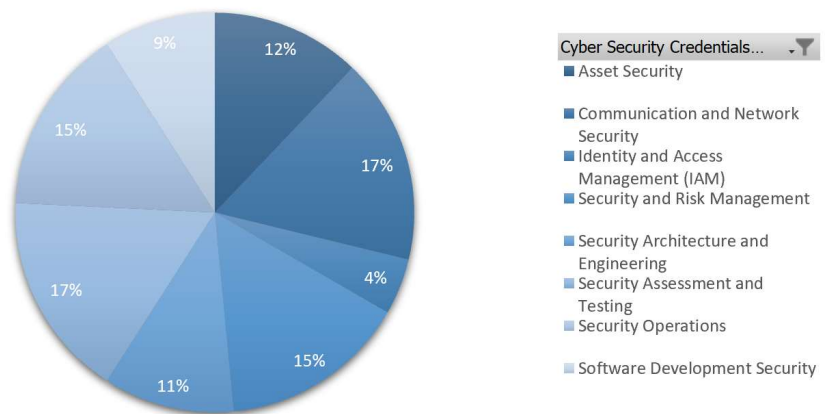
The duration of courses at higher education providers varies greatly, from 19 weeks (in the case of an advanced diploma) to 416 weeks (a combined undergraduate degree), with Masters and Doctoral degrees occupying a middle-point between these.



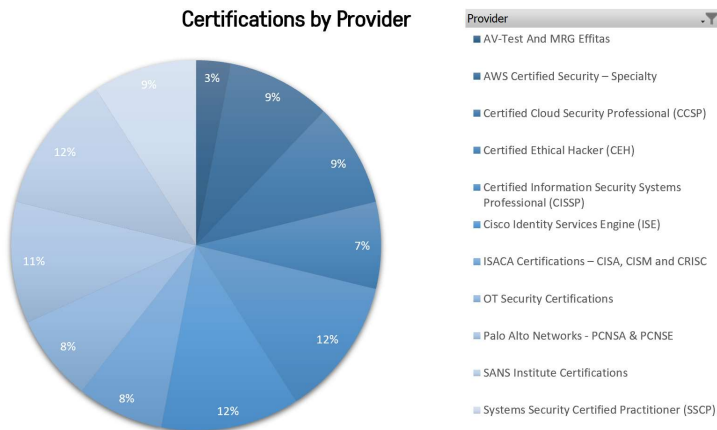
Micro-Credentials

Provider	Cyber Security Credentials By Certification	Certified Information Security Systems Professional (CISSP)	AWS Certified Security – Specialty	Certified Cloud Security Professional (CCSP)	ISACA Certifications – CISA, CISM and CRISC	OT Security Certifications	Palo Alto Networks – PCNSA & PCNSE	Systems Security Certified Practitioner (SSCP)	Certified Ethical Hacker (CEH)	SANS Institute Certifications	Cisco Identity Services Engine (ISE)	AV-Test And MRG Effitas
Certified Information Security Systems Professional (CISSP)	Security and Risk Management	x	x	x	x	x	x	x	x	x	x	
Certified Information Security Systems Professional (CISSP)	Asset Security	x	x	x	x		x	x		x	x	
Certified Information Security Systems Professional (CISSP)	Security Architecture and Engineering	x		x		x	x	x		x	x	
Certified Information Security Systems Professional (CISSP)	Communication and Network Security	x	x	x	x	x	x	x	x	x	x	x
Certified Information Security Systems Professional (CISSP)	Identity and Access Management (IAM)	x								x	x	
Certified Information Security Systems Professional (CISSP)	Security Assessment and Testing	x	x	x	x	x	x	x	x	x	x	x
Certified Information Security Systems Professional (CISSP)	Security Operations	x	x	x	x	x	x	x	x	x	x	
Certified Information Security Systems Professional (CISSP)	Software Development Security	x	x				x		x	x	x	

Certification Type



Certifications by Provider



ADVERTISED VACANCIES

iii. Advertised vacancies

ANZSIC (division) and ANZSCO (code)

Age

Gender

Geographic location (State/Territory/Commonwealth -national)

Comparative overview: US/UK/GER/NZ as per working taxonomy in terms of employment needs met / oversupply / shortage

TOP CYBERSECURITY JOBS (To be populated based on data pull request)

iii. Advertised vacancies

Total job openings (The number of advertised cybersecurity job roles at national, state-wide and city-wide levels)

The most-advertised job titles in a selected location (Cyber Seek AU ALL)

- Business Intelligence Analyst
- Security Architect
- Cyber Security Analyst
- Security Engineer
- Network Engineer

ANZSIC (division) and ANZSCO (code)

Age

Gender

Geographic location (State/Territory/Commonwealth -national)

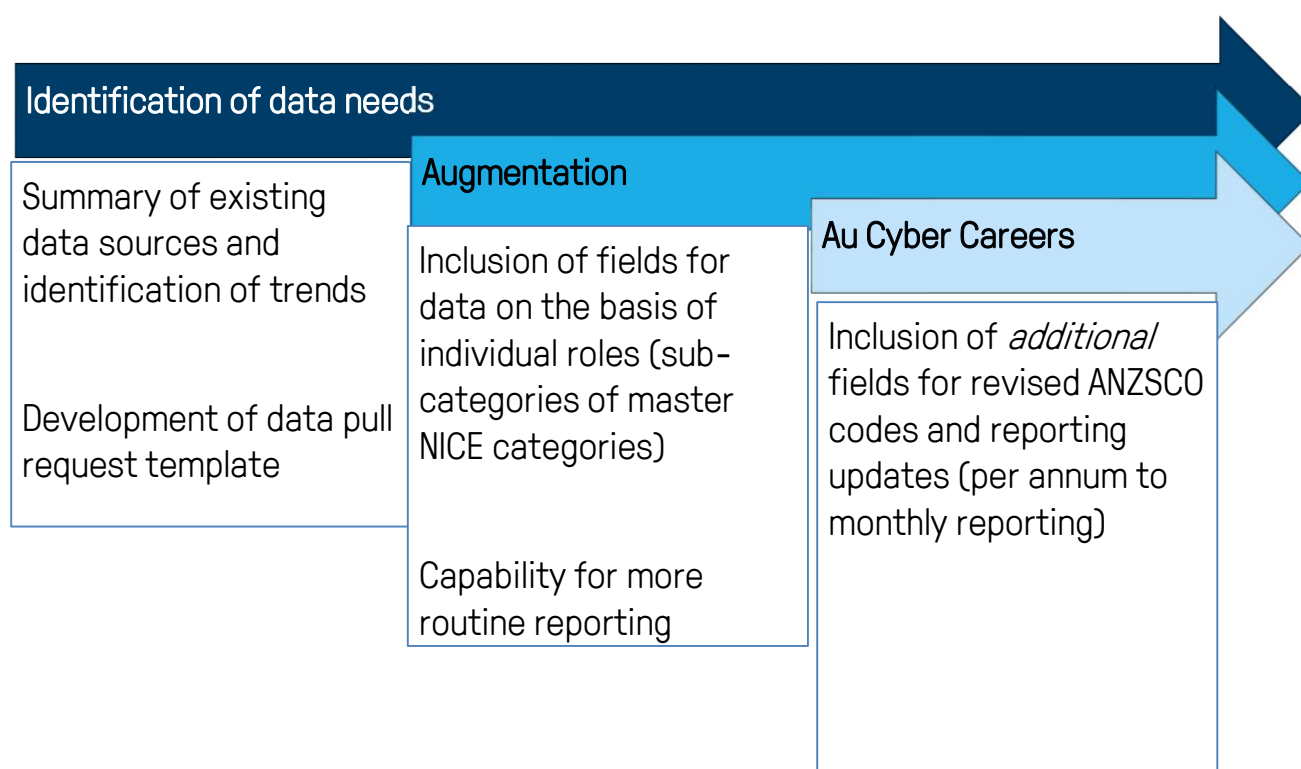
Comparative overview: US/UK/GER/NZ as per working taxonomy in terms of employment needs met / oversupply / shortage

FORWARD GROWTH/FORECASTING: PHASE 2

Forecasting model: Phase two of AuCyberSeek

We envisage the forecasting model, subject to stakeholder input, being developed and enacted in a three stage process, as outlined below. This encompasses the current phase of data analysis, initial augmentation, to improve the quality, breadth and availability of data and, finally, a full optimization, which maps the NICE Categories against the revised ANZSCO codes. It is anticipated that these will be announced in November 2021.

This will enable data to be ingested, digested and modelled over shorter timeframes, including months, which will make comparisons easier, including by location, field of specialization and other relevant criteria.



APPENDIX ONE: REFERENCES/DATA SOURCES

Source	Nature of data	Data fields	Frequency
<i>IT Security Consulting in Australia</i> (IBIS World)	Primary and Secondary	- Jobs - Sector growth - Dominant companies	Annual
<i>Digital Census 2020</i> (AustCyber)	Secondary	Aggregate number of cyber security jobs (Australia-wide)	Annual
<i>Vacancy Report June 2021</i> (National Skills Commission)	Primary	ANZSCO code level	Quarterly
<i>Sector Competitiveness Plan</i> (AustCyber)	Primary	Aggregate number of cyber jobs (Australia wide, and State-State)	Annual

APPENDIX TWO: DATA REPORTING TEMPLATE

1. DISER requester details	
Contact name	
Position	
Division/area	
Physical Address	
Telephone number	
Email	
2. Data specification and use	
Data description	Please outline the nature of the data you are seeking. Some factors you might wish to consider include: • Data type (i.e. # of new advertised jobs within x category area) • Level of granularity of data (i.e. aggregated or further defined) • Timeframe of data (i.e. from 2019-2021) • Geospatial parameters (i.e. within the State of NSW, or National)
Frequency of data provision	How frequently will the data need to be provided? ☐ Once off ☐ Quarterly
Uses(s) of the data	<u>Uses</u> Please describe how the data will be used. This might include, for example: preparing detailed briefing notes or supporting evidence for New Policy Proposals. <u>Publication</u> How long will the data be stored for and how, if at all, will it be published?
Will the data be integrated, matched or in any other way compared with existing data sets?	☐ Yes. (if so, which ones, please specify: _____) ☐ No
Data Access	Within your Department, who will have access to the data we generate? For example, will it be IT contractors, policy officers, procurement officers or others?
Relevant conflicts of Interest	Are there any known or potential conflicts of interest in terms of who will obtain the information, or any third parties who may have access to it?
3. Purpose of request	
What is the reason for this data request?	For example, what initiative is this part of, is this sought as part of a response to a Ministerial Briefing request, Question on Notice, Request for Proposals, or to support broader policy development purposes?
Data provision date	When is this data required by?