www.pwc.com.au

Cyber Security Cross-Sector Project

Case for Change

Table of Contents

1. Administrative Information

Name of the Cross Sector Project	Cyber Security
Name of the lead Skill Service Organisation	PwC's Skills for Australia
Project webpage address	www.skillsforaustralia.com/cross-sector-projects /cyber-security
Members of Project Reference Group (PRG)	Attachment A
Name of the training package(s) and qualifications, skill sets and units of competency (if known) impacted by proposed cross sector training product components	Attachment B
Stakeholder Consultations	Attachment C

2. Executive Summary

The Australian Industry and Skills Committee (AISC) has taken the opportunity to strategically address current and future skills needs across multiple industries through eight cross sector projects. These eight common skills areas have been identified by various Industry Reference Committees (IRCs) in their Industry Skills Forecasts and proposed Schedules of Work, which set out the emerging industry trends, skills needs and training priorities over a four year period, for a particular industry. The aim of these cross sector projects is to develop training package components that address eight common skills areas across multiple industries in a coordinated and efficient way.

Cyber Security cross sector project: purpose, scope and objectives

The Cyber Security cross sector project, led by PwC's Skills for Australia, is undertaking the review of current and emerging developments in Cyber Security skills, particularly in relation to data confidentiality, protection and privacy, and identify related skills needs shared by multiple industry sectors. The purpose of this project is to provide an evidence-based case and industry support for developing common training units to be used across multiple training packages. This project also aims to better understand what these units might look like, how they might be delivered, and what benefits or risks need to be considered with any potential changes to existing Vocational Education and Training (VET). It is expected that this project will result in a significant reduction in duplication across the national VET system, and help to deliver a future fit Cyber Security workforce to organisations across multiple industries.

The Cyber Security Project Reference Group (PRG), consisting of IRC members, is responsible for the direction of this cross sector project and provide guidance, governance and make decisions based on the industry and stakeholder groups they represent.

Relevant sectors/industries impacted

Due to the broad reaching nature of Cyber Security in an increasingly digital world, there is a long list of industries which could potentially benefit from improved Cyber Security related training products (see Attachment B for a more detailed overview of potentially impacted training packages). Some of the major impacts will be experienced by industries including information and communications technology, financial services, business services, mining, automotive and health. IRC approval and support was sought from all IRCs by collaborating with their relevant Skills Service Organisations (SSOs).[1]

Summary of proposed changes:

The five main changes proposed are as follows:

1. Develop 2 new basic units for 'Cyber Security Awareness' (one at a nominal Certificate II level and another at nominal Certificate III level). These would apply to a broad range of training packages, with the aim of improving general Cyber Security awareness among workers. The unit at nominal Certificate II level will target workers at lower levels of a

[1] At the time of submission of the Cyber Security Case for Change, we received approval and support from 17 IRCs, including those identified as potentially impacted training packages (Information and Communications Technology; Business Services; and Property Services).

business; the unit at nominal Certificate III level will target workers in managerial or higher levels of a business.

2. Develop a 'Cyber threat intrusion/detection and response' skill set that could form a specialisation element of Cyber Security at a nominal Advanced Diploma level. This proposed skill set could have 4 new Units of Competency that could also be drawn upon as electives across a broad range of training packages to bolster existing qualifications.
3. Potentially replace 6 existing Units of Competency related to Risk Management and Cloud Computing in current training packages (residing in ICT, CPP and BSB training packages) with 2 new common units, in order to remove obsolete and/or duplicated content. These 2 new common Units of Competency will be separate from those created in the skill set outlined in recommendation #2.
4. Identify Units of Competency that already exist and could be imported into other training packages as electives to improve portability. Our analysis has identified 35 potential Units of Competency currently housed within the Information and Communications Technology training package. The aim of this identification exercise is to improve the flexibility of existing units for potential broader use across the training system.
5. Identify existing accredited units in Cyber Security and determine whether there are industry agnostic common units that could be brought into the national VET system.

Given that the purpose of this project is to identify and develop common training products that can be used across a range of industries, a Cyber Security qualification was not recommended at this stage of the project, as it requires an industry specific background in ICT related disciplines. However, it is expected that the proposed skill set would allow learners to supplement an already existing occupation or qualification and generally increase an individual's Cyber Security skills so they could more effectively complete their primary role.

3. *The Case for Change*

Sector/Industry drivers of change

This Case for Change is proposed in response to the following industry drivers identified in desktop research and stakeholder consultations:

Shortage of adequately trained Cyber Security individuals in the Australian workforce - over 85% of Australian IT professionals believe there is a critical shortage of domestic Cyber Security skills.[2] The same group of professionals believe that this will lead to 17% of Cyber Security roles remaining unfilled in the future. Furthermore, Australia has seen an increase in cyber attacks,[3] which is likely to increase the demand for qualified Cyber Security professionals.[4]

Lack of industry-aligned Cyber Security training - there is an opportunity for the Information and Communications Technology sector, and the VET sector more broadly to design courses that will help to address the existing Cyber Security skills shortage.[5] This sentiment was echoed by industry representatives throughout our consultations and survey, with these individuals also suggesting that new common units would provide opportunities for workers across multiple industries to reskill or upskill in order to meet industry demand.[6] For example, Box Hill Institute in Victoria has developed accredited courses in Cyber Security in conjunction with the private sector and is being considered for adoption by other states as a possible course model to teach Cyber Security skills.

[2] Center for Strategic and International Studies, *Hacking the skills shortage* (Intel Security, 2016) <https://www.mcafee.com/au/>.

[3] 114,000 reports of cybercrime have been registered with the Australian Cybercrime Online Reporting Network (ACORN) since 2014 and 23,700 just in the past six months. See Patrick Durkin, *Cyber attacks 'rife' in Australia* (Australian Financial Review, 2 July 2017) <http://www.afr.com/technology/cyber-attacks-rife-in-australia-20170629-gx17j9>.

[4] Southern Cross University, *Rising demand for IT professionals with cybersecurity skills* (2017) <https://online.scu.edu.au>.

[5] Raveena Grover, *ACS announces Director of Cyber Resilience* (ASC News, 2017) <https://ia.acs.org.au/>.

[6] PwC's Skills for Australia, Cyber Security Cross Sector Project Industry Survey (base: 72 responses as of 26.09.2017), Interview and Focus Group Responses (base: 47 responses as of 02.10.2017).

Current and emerging developments in skills needs

Top-down analysis based on industry trends and skills needs

Through extensive industry consultation, the following Cyber Security skills needs were identified and these are applicable across multiple sectors and industries.

1. A need for basic Cyber Security skills: employers and training providers we spoke to indicated a high demand for better Cyber Security awareness skills among business and ICT users. Other skills recognised as vital for a Cyber Security professional included effective communication and critical problem solving skills.

2. A need for more advanced Cyber Security skills: stakeholders from a number of industries (including automotive, health, finance, ICT and manufacturing, to name a few) identified a number of advanced Cyber Security skills needs:

- **Cyber threat intrusion/detection and response skills**, to monitor the network traffic, manage and respond to unusual or suspicious activity on the network to protect a business from cyber attacks. This advanced Cyber Security skill would include a background understanding of analytical and computer network skills, knowledge of monitoring applications and toolsets, along with basic knowledge of cyber threats.
- **Network and web application vulnerability assessment skills,** to identify security vulnerabilities on the network, web applications and produce recommendations to remediate identified security issues across existing infrastructure. This advanced Cyber Security skill includes understanding of computer networks and programming skills.
- **Cyber risk assessment skills**, to identify cyber risks and ultimately help to reduce Cyber Security incidents in organisations. This advanced Cyber Security skill includes knowledge of Risk Management and security standards such as ISO27001.
- **Managing and monitoring network access control skills,** to protect a network from internal or external Cyber Security threats and incidents by applying network security controls such as intrusion preventions systems, firewalls etc. This advanced Cyber Security skill includes knowledge of installing and monitoring firewalls, intrusion prevention systems etc.
- **Cyber Security incident response skills**, to conduct cyber and forensic investigations such as computer memory analyses, network packet capture or malware analysis. This advanced Cyber Security skill includes analytical skills with proven knowledge in IT security operations, risk management and vulnerability management.
- **Secure software development skills,** to help guard against security vulnerabilities and data breaches in software or software code. This advanced Cyber Security skill includes programming skills and basic Cyber Security awareness.

Bottom-up analysis of existing training package components

We conducted a broad initial search for unit titles on training.gov.au using the keywords “Information Technology”, “cyber” and “security”, and identified 193 units of competency.[7] We further filtered the Units of Competency to identify those specifically related to Cyber Security by using additional keywords including ‘encryption’, ‘network security’, ‘risk’, ‘cloud’ and ‘vulnerability’; a total of 77 Units of Competency were identified.[8]

Units that could be removed because of duplication

Of these 77 Units of Competency, we identified 6 units that offer similar skills and knowledge (based on the unit elements and the skills outcomes) to meet industry needs and could potentially be collapsed into proposed 2 new common units to reduce duplication across training packages. Given this proposed change would have a direct impact on a number of training packages, a careful review of these existing 6 units (residing in Information & Communications Technology, Property Services and

[7] Australian Government Department of Education and Training, See ‘*Nationally recognised training search portal*’, (2017) <https://training.gov.au/Home/Tga>.

[8] At the time of writing of this Case for Change, the Department of Education and Training was working to develop and launch an algorithm to assist with content analysis of training package components. Depending on when this is made available, more sophisticated unit analysis may be possible and therefore may alter the number of potential units identified in this Case for Change.

Business Services training packages) would need to be completed, accompanied by further targeted consultation. To see a more detailed breakdown of this mapping exercise of potential superseded units to proposed new Units of Competency, see Attachment B.

Units that could be imported into various training packages

Based on our desktop research, we also found 35 Cyber Security related Units of Competency that currently reside in different training packages (including Information & Communication Technology, Property Services and Public Sector training packages) and could be adopted by other training packages (such as Business Services, Maritime, Financial Services, Community Services and Culture and Creative Arts) as electives. For example, existing units relating to network security that currently sit in the ICT training package have been drafted in an industry agnostic manner, and could be adopted by other training packages as electives. Given this proposed change would have a direct impact on a number of training packages, a thorough review of these 35 Units of Competency would need to be completed, followed by further targeted consultation. More detail regarding these units can be found in Attachment B.

Opportunities to promote occupation mobility and for modernising sector/industry specific units, qualifications or skills sets

It is clear from our top down and bottom up analysis that there is opportunity to develop common Cyber Security units that equip learners with general Cyber Security related skills that could be transferable to any industry, occupation or level in an organisation. These industry agnostic, common units then serve two purposes: common units that can easily be adopted by multiple training packages and contextualised for industry; and common units that can help identify existing units for review or removal to address obsolescence and duplication in training packages.

Proposed changes

#	Change	Rationale
1	Develop 2 new basic units for 'Cyber Security Awareness' (one at a nominal Certificate II level and another at nominal Certificate III level) to apply to a broad range of training packages. The unit at nominal Certificate II level will target workers at lower levels of a business; the unit at nominal Certificate III level will target workers in managerial or higher levels of a business	The Australian Government along with the private sector is keen to improve national Cyber Security awareness and cyber resilience to ensure all Australians understand the risk and threats that exist (and are continually evolving) in cyberspace. Currently, there is no Cyber Security awareness program at a vocational level that can be drawn upon as elective across a broad range of training packages. This new common unit will allow learners to understand the importance of Cyber Security in their daily life. Further consultation will be required, but it is expected that learners completing these units will be able to recognise confidential information and handle it more securely using generic security controls such as applying strong passwords etc (Cyber Security Awareness unit - Cert II). Executives will be able to understand responsibilities related to Cyber Security and develop strategies to mitigate cyber risk in the organisation (Cyber Security Awareness unit - nominal Certificate III). ... continued over page

#	Change	Rationale
2	Develop 4 new units to form a skill set in 'Cyber threat intrusion/detection and response'. Further consultation will be required, but these units could include: 1. Network architecture review 2. Advanced analysis and network Forensics 3. Intrusion Detection System Fundamentals 4. Advanced Intrusion Detection System concept These units could be written at nominal AQF Level 6.	Stakeholders identified a number of advanced Cyber Security skills needs, as noted in section '*Current and emerging developments in skills needs*', but identified 'Cyber threat intrusion/detection and response' as the most critical and immediate skills gap facing the current Cyber Security workforce in Australia. This skill set is designed to address this current skills gap, recognising that there is an opportunity to later develop skill sets in the remaining skill areas noted in above section or later develop a qualification in Cyber Security covering the remaining skills identified by the stakeholders. For this advanced Cyber Security skill, learners might benefit from a background of analytical and computer network skills, knowledge of monitoring applications and toolsets, along with basic knowledge of cyber threats. Further consultation will be required, but it is expected that learners completing these units will be able to deal with emerging cyber attack techniques and vulnerabilities to the network and business environment.
3	Develop another 2 new common units, to potentially replace 6 existing Units of Competency related to Risk Management and Cloud Computing (residing in ICT, CPP and BSB training packages). These 2 new common Units of Competency will be separate from those created in the skill set outlined in recommendation #2	We identified 6 units containing obsolete and/or duplicative content related to Risk Management and Cloud computing (residing in ICT, CPP and BSB training packages). These could potentially be compressed into 2 new common units: - Implementation of Risk Management - Cloud Computing in Business Analytical skills and basic knowledge of computer operating systems are the prerequisites for these units. Further consultation will be required, but it is expected that learners completing these units will be able to implement a Risk Management framework in their organisation and manage Cloud Computing strategies for their business.
4	Identify Cyber Security related Units of Competency that already exist so that they can be transferred into other training packages as electives.	Our analysis has identified 35 potential Units of Competency that are currently housed within the Information and Communications Technology training package at different nominal levels. The aim of this identification exercise is to improve the flexibility of existing units for potential broader use across the training system. More consultation may be required, but these units could be drawn upon as prerequisites as outlined in proposed change #2. For more information: please see Attachment B. Basic knowledge of computer networks and operating system might be considered a prerequisite for these units.
5	Identify existing accredited units to determine whether there are common units that could be brought into the national VET system.	The purpose of this activity is to identify existing accredited units in Cyber Security related qualifications that are currently helping to address the cyber skills shortage. Where appropriate, insights from these units could be introduced into the national VET system as well. Coding skills along with strong knowledge of computer networks and operating systems are likely to be prerequisites for these units.

Total proposed changes

Summary of proposed changes to training products	**Number of training products**		
	New	**No Change***	**Potentially remove**
Proposed new skill set			
New skill set to be created (see ‘Proposed changes’ table, Item 2)	1		
Proposed changes to units			
New units to be created (see ‘Proposed changes’ table, Items 1, 2, 3)	8		
Existing units to be reviewed for duplication and possible removal (see ‘Proposed changes’ table, Item 3)			(6)
Identify units to import into other training packages (see ‘Proposed changes’ table, Item 4)		35	
Identify accredited units and potentially import into national VET system (see ‘Proposed changes’ table, Item 5)		13	
Net result of proposed training product changes	**2**		

* Units that already exist in other training packages and could be applicable to multiple industries.
Numbers in parentheses indicate units for potential removal.

Implementation advice and considerations

Listed below are some implementation considerations to support these proposed changes. For more detail, please refer to Attachment B.

- ***Continue to engage IRCs and SSOs to identify additional existing units that are duplicated and could be removed*** - we would suggest to seek further advice from IRCs regarding the potential units they consider might be similar and could be replaced by proposed new Cyber Security Units of Competency.
- ***Consider options for where these new potential Cyber Security units of competency could be located*** - we see a few options for consideration, including:
    - Form a new generic training package to accommodate proposed Cyber Security units; or
    - Use an existing training package, such as the ICT Information and Communications Technology training package given the close technology component to Cyber Security.
- ***Continue to engage IRCs and SSOs to consider proposed new Cyber Security units for importation into their training package as electives and replacements for duplicated units*** - Extensive consultations have taken place to justify the proposed changes in this report (see Attachment C). However, in order to ensure that the proposed new units will be taken into various training packages as potential electives or replacements for duplicated units, we will need to continue to engage with IRCs and work with SSOs throughout the training product development process. For a detailed overview of how superseded units map to proposed new generic Units of Competency, see Attachment B.
- ***Consider implications for upskilling trainers who will teach and contextualise common units*** - The development of common units will necessitate greater emphasis on contextualisation, and this may have implications for the upskilling of trainers who will teach these units and/or the companion volumes that accompany the proposed new units.
- ***Consider funding arrangements and differences between state/territory jurisdictions*** - Traditionally, skill sets do not attract government funding, and some stakeholders suggested that this might impact uptake of the proposed skill set. Nonetheless, a large part of the utility of these units is their application to other training packages in the form of electives.

4. Industry Support for Change

Consultation approach

A key objective of our stakeholder consultations was to achieve breadth of representation from industries, geographic locations, and stakeholder categories. To do this, we leveraged our existing PRG and IRC member networks, the broader PwC network, other SSO and Department contacts, training providers, subject matter experts and thought leaders. We also consulted with additional contacts who were referred to us through the course of this cross sector project, pushing content through these networks and social media channels (e.g. LinkedIn, Twitter, industry newsletters, PwC's Skills for Australia website subscribers).

Industry views were captured via stakeholder interviews, focus groups and responses to an online public survey. The method and scale of stakeholder consultation undertaken in building the Case for Change is outlined in Attachment C – Stakeholder consultation method and scale.[9] In summary, there were 132 responses through our consultation channels, representing 27 different industries. Furthermore, all states and territories contributed at least in one form to the consultation process. This provides strong evidence of effective consultation, engagement and collaboration across a diverse spread of sectors and industries. Assuming this Cyber Security Cross Sector Project progresses to a second phase of work (i.e. a Case for Endorsement), then additional targeted industry consultations will be conducted to further support the development of the proposed training products.

In seeking support and approval for this Case for Change, PwC's Skills for Australia reached out to all IRCs, including those that were materially impacted by the proposed changes, and all State/Territory Training Authorities (STAs). This involved sharing a two-page summary 'Briefing Paper', a draft Case for Change and an online survey for feedback. At the time of finalising this Case for Change, we had responses from 17 different IRCs; and feedback from 4 STAs, who had only minor comments, which we took as a strong signal of industry support for the Cyber Security Case for Change.[10]

Cross-sectoral support for proposed change

We consistently heard across all forms of consultation that current vocational training is not adequate in equipping workers with Cyber Security related skills. When asked how well current vocational education and training equips learners with the Cyber Security skills they need in industry, only 14.5% of survey respondents responded 'very well' or 'extremely well'. This sentiment was consistent across all industries and stakeholder types.

Stakeholders were supportive of a proposition to develop a skill set relating to Cyber Security skills. More specifically, it was found that the proposed skill set in Cyber Threat and Intrusion was the most appropriate training product to propose at this stage of the project. This skill set would allow learners to supplement an already existing occupation or qualification and generally increase an individual's Cyber Security skills so they could more effectively complete their primary role.

Throughout this phase of the Cyber Security cross sector project, stakeholders from leading industry associations expressed hesitations about creating a vocational qualification in 'Cyber Security'. They argued that Cyber Security related skills are considered to be highly specialised and require a background in ICT related disciplines. Even though a qualification is not recommended at this stage of the Cyber Security Cross Sector Project, it should not be ruled out indefinitely. Further targeted consultations and collaboration may be required in the second phase of work, especially with representatives with a background in Information and Communications Technology, to test whether a

[9] See also PwC's Skills for Australia, *Public Paper - Cyber Security Cross Sector Project* (2017) <https://www.skillsforaustralia.com/cross-sector-projects/cyber-security/>, 17-18.

[10] As at 28 November 2017, we received IRC approval and support from 17 IRCs, including those identified as potentially impacted (Information and Communications Technology; Business Services; Property Services) and other IRCs (Agriculture and Production Horticulture; Aquaculture and Wild Catch; Automotive Heavy Vehicle; Civil Infrastructure; Coal Mining; Construction, Plumbing and Services; Culture and Related Industries; Electricity Supply Generation; Financial Services; Maritime; Meat; Racing; Rail; and Sustainability). As well, feedback was received from 4 STAs (Australian Capital Territory Government; New South Wales Department of Industry; Department of Education and Training Queensland; and Department of Education and Training Victoria), with only minor suggestions and in support of the Cyber Security Case for Change.

more technical Cyber Security related qualification could be developed and where this qualification might sit.

A number of issues were raised by stakeholders and these were mainly supporting considerations that need to be taken into account for successful implementation and delivery of these common training package components.

Issues identified by stakeholders

- **Strong industry demand for more hands-on/practical experience –** multiple stakeholders suggested that courses or qualifications in Cyber Security often lack grounding in real-world scenarios and experience. This was perceived to lead to poor handling of cyber related incidents in the workplace. Hands-on/practical experience opportunities include work placements and projects or assignments involving 'real world' client problems.
- **Gaps in current training units –** stakeholders across different industries indicated that current vocational training in Cyber Security skills is inadequate and, as an example, stakeholders cited the fact industry certification is not an essential requirement of cyber security professionals. Consequently, many employers need to spend time and money to train their Cyber Security workforce.
- **Balancing technical Cyber Security skills with skills in business, communication and teamwork –** employers and training providers acknowledged that one of the challenges with the current Cyber Security workforce is finding the right balance between adequate technical Cyber Security skills with effective business understanding, communication, and interpersonal skills. This was perceived to contribute to a lack of skill in translating identified cyber threats into business actions and outcomes.
- **Duplication of units –** currently there are 6 very specific units that serve similar purposes within the ICT Information & Communications Technology, BSB Business Services and PSP Public Sector training packages. This can create confusion about learning options when trying to select from these units, and also presents an opportunity to streamline some of these units to reduce duplication of training. For more information see Attachment B.
- **Potential risk of obsolescence if new training products are created in Cyber Security related skills –** Some stakeholders noted that there was a risk that the proposed new training products could quickly become outdated due to the rapid pace of technological change and relatively slower process of training product development and review cycles. We see two methods to mitigate this risk. First, draft units in a more generic nature that allows training providers to refer to the most current examples and applications of Cyber Security related skills. Second, conduct more frequent reviews of Cyber Security related training products to ensure that training materials keep up with advancements in Cyber Security related disciplines. Stakeholders were still in agreement that, despite this risk, the benefits of updating vocational training to include Cyber Security related skills far outweighs the negative prospect that they may become obsolete for a short period of time before they are updated again.
- **Consider funding arrangements and differences between state/territory jurisdictions –** traditionally, skill sets do not attract government funding, and some stakeholders suggested that this might impact uptake of the proposed skill set. Nonetheless, a large part of the utility of these units is their application to other training packages in the form of electives.
- **Upskilling trainers to deliver proposed new training products -** trainers may need to be upskilled if they are to successfully deliver the proposed new training products. This in turn requires consideration of funding or other support that may be required to encourage professional development of trainers.

Sensitivities and/or dissenting views

One dissenting view that was identified by a small number of training providers was that the general nature of industry agnostic units can make it difficult for learners to understand their importance in the mainstream courses. In order to maintain learner interest, we would propose that each unit incorporates a practical component and is flexible enough for training providers to contextualise the unit to each industry.

In addition, there is a possibility that accredited courses in Cyber Security in Victoria could be adopted in other states like New South Wales and South Australia. This adoption would help to address Cyber Security workforce shortages, but might have financial implications for each state as these accredited courses have private copyright and are developed with private funding. The owners of these accredited courses has the discretion to make them available in public domain or may charge fees or conditions for access.

This proposed skill set would help to address the current skills gap; however, it does not rule out the development of additional training products in the future. Upon subsequent reviews, there might be opportunities to develop additional skill sets or qualifications to cover more advanced Cyber Security skills.

5. Impact of Change

Throughout our consultation process, we asked our stakeholders to comment on the potential impacts of change (including risks and benefits), as outlined below.

Stakeholder	Impact
Industry wide	● Organisations with a specialised cyber workforce will be able respond more effectively to sophisticated cyber attacks. If cyber skills are not improved, it could lead to an embarrassing data breach.[11] ● Reduced cyber risk in operational technology systems such as cars, traffic lights, mining systems.. ● Increased security of ATM, credit card and mobile banking applications will foster trust of Australia's financial system ● Confidence in the Cyber Security/digital technologies will open new business opportunities and boost future economic growth in Australia
Industry/ Employers	● Address current Cyber Security skills shortages ● Improve alignment of training products to the needs of industry ● Increase relevance of skills to organisations ● Increase efficiency in cyber operations ● Increase staff retention
Registered Training Organisations	● Increase enrolments and completion rates ● Improve efficiency of the training system through the removal of duplicate/obsolete units of competency and qualifications ● Increase flexibility in training product offerings
Learners	● Increase awareness of Cyber Security issues ● Increase an individuals' ability to recognise and solve problems before they become an issue ● Improve job opportunities for learners in Cyber Security ● Increase in contemporary skills and knowledge in Cyber Security

Implications of not implementing proposed changes

Stakeholder	Impact
Nationwide	● Cyber threats may continue to escalate in Australia, posing a clear national security risk ● Economic growth and stifling innovation would be inhibited ● Loss of international competitiveness if Australia fails to act or is slow to act

[11] Riia O'Donnell, Cybersecurity skills gap widens, despite clear demand for experts (5 October 2017) <http://www.hrdive.com>

Industry/ Employers	● Fewer skilled Cyber Security professionals ● Escalating shortage of future Cyber Security talent ● Increased financial cost to organisations due to cyber attacks such as data breaches and ransomware ● Significant financial cost, particularly to small businesses, as a result of cyber attacks resulting in outages/disruptions to operations
Registered Training Organisations	● Training packages not aligned to industry needs may produce a risk of substandard training packages and could further reduce enrolment in cyber courses.
Learners	● Less job opportunities ● Falling prey to cyber criminals due to lack of Cyber Security awareness

Advice on linkages with other cross-sector projects

As the cross-sector projects address skills needs across all industries, it is important that any crossover between projects is identified. The below table lists the projects that have been identified as having possible links to the Big Data, Teamwork and Communication and Digital Skills cross sector project, and how that link is being addressed.

Cross-Sector Project	Lead SSO	Link
Big Data	PwC's Skills for Australia	There was strong support for the development of training which covers the topic of 'Data Analysis for Security Information and Event Management (SIEM) platform and data security'. This presents an opportunity for collaboration with the Big Data project to develop relevant industry agnostic unit(s).
Teamwork and Communication	PwC's Skills for Australia	One of the themes we heard from our consultations was that it is important for people to be able to communicate effectively in cyberspace in order to translate cyber risks into a business imperative. This observation might not directly change the development of Cyber Security units, but it does highlight the importance of the inclusion of communication skills for all learners.
Digital Skills (previously Coding)	Innovation and Business Skills Australia (IBSA)	Various programming languages are heavily used in Cyber Security related disciplines (e.g. Python and SQL) for optimising their security processes.

How the proposed changes advance the project's priorities

The AISC has established the cross sector projects to address skills shortages that are common across a variety of industries. This Case for Change has proposed the creation of a Cyber Security related skill set and several Units of Competency to ensure that vocational learners across a variety of industries can access up-to-date Cyber Security related training. To ensure that the new training materials are current and relevant, continued cross-sectoral input would be sought to address specific skills shortages. In addition, another one of the aims of the AISC was to minimise unit duplication in the VET sector. To address this, we have proposed a review of 6 Cyber Security related units that could possibly be replaced by 2 proposed new common units.

Estimated timeframes for implementing the proposed changes

Assuming the Case for Change is approved by the AISC at the February 2018 meeting, it is anticipated that implementation of the proposed changes could take place by November 2018, at which point a final Case for Endorsement would be ready for submission to the Department of Education and Training. This would allow time for a further round of targeted consultations to support the drafting of new training products, review existing units and design and implement updates to these, and draft a supporting Case for Endorsement. We anticipate that this process would take approximately 9 months to complete from the date of approval of this Case for Change.

Implementing the COAG industry and Skills Council reforms for Training Packages

The table below identifies how the Case for Change will address the focus areas agreed upon by the CISC skills session in November 2015.[12]

Reform	Evidence of reform being addressed
Ensure obsolete and superfluous qualifications from the training system	The creation of new common units and skill sets will help identify existing units across multiple training packages that could be removed due to duplication and obsolescence.
Ensure that more information available about industry's expectations of training delivery	Companion Volumes will be released with the proposed new training materials, containing information about industry's expectations of training delivery. Which Companion Volumes get updated will depend on where these common units will be housed.
Ensuring the training systems better supports individuals to move easily from one related occupation to another	The development of industry agnostic Cyber Security related units of competency will allow learners to apply these skills in various roles and across various industries. Furthermore, it may act as a pathway into tertiary education in related fields such as Computer science or information security.
Improving the efficiency of the training system by creating units that can be owned and used by multiple industry sectors and housing units in a work and participation bank	Similarly, industry agnostic units of competency could be easily drawn into a wide range of training packages to benefit many industry sectors. See Attachment B
Fostering greater recognition of skill set	A key proposed change is to develop a skill set in Cyber Security. This will serve to increase the use and recognition of skill sets in VET more broadly
Ensures that new training courses can be developed as quickly as industry needs them and available to support niche skill needs	Learners who are enrolled in accredited courses that import the proposed Cyber Security related units of competency will benefit from training which has been updated to meet industry needs.

This Case for Change was agreed to by the Cyber Security PRG.

WAYNE RALPH WILSON 30/11/'17

Cyber Security PRG Chair Signature of Chair Date

[12] *Communiqué for the COAG Industry and Skills Council Meetings Skills Ministers*, (Communiqué, 2015) <https://docs.education.gov.au/>.

Attachment A: Members of the Cyber Security Project Reference Group

Industry Reference Committee (or Subject matter expert)	Name	Organisation, Position
Subject matter expert	Bill Galvin	Tourism Training Australia, Chief Executive
Information and Communications Technology IRC (PwC's Skills for Australia)	David Masters	Microsoft, Corporate affairs Manager
Information and Communications Technology IRC (PwC's Skills for Australia)	Emma Broadbent	Cisco Social Innovation Group, Regional Manager ANZ & Pacific Islands
Local Government IRC (SkillsIQ)	Heidi Loncar	City of Albany, HR Coordinator
Property Services IRC (Artibus Innovation)	John Fleming	Australian Security Industry Association of Australia, General Manager
Community Sector and Development IRC (SkillsIQ)	Katina Jones	Equals International, Chief Executive Officer
Automotive Strategic IRC (PwC's Skills for Australia)	Mark Harper	Utilities Engineering Electrical and Automotive Training Council, Industry Consultant Automotive and Engineering
Maritime IRC (SkillsIQ)	Mark Shannon	Serco Asia Pacific, Contract Director
Business Services IRC (PwC's Skills for Australia	Michael Magelakis	SSMI Group, Chief Executive Officer
Automotive Strategic IRC (PwC's Skills for Australia)	Peter Blanshard	Institute of Automotive Mechanical Engineers, CEO
Culture and Related Industries IRC (PwC's Skills for Australia)	Peter Mousaferiadis	Cultural Infusion, Founder and Chief Executive Officer
Rail IRC (Australian Industry Standards)	Russ Evans	Rail Industry Safety and Standards Board, General Manager
Subject matter expert	Sarah Kauppinen	Department of Defence
Transmission, Distribution and Rail IRC (Australian Industry Standards)	Stuart Johnston	Energy Networks Australia, Executive Director - Assets and Network Transformation
Financial Services IRC (PwC's Skills for Australia)	Wayne Wilson	KnowIT Group, Chief Executive Officer

Attachment B: Training package components to change

IRC Name	SSO with Responsibility	Training Package Code	Training Package Name	Training Product Code	Training product name (Qualification, skill set, unit of competency)	Review Status (New or updated)	Change required
Cyber Security Cross Sector Project	PwC's Skills for Australia	TBD	TBD	TBD	Cyber threat intrusion/detection and response	New skill set	Draft new skill set
Cyber Security Cross Sector Project	PwC's Skills for Australia	TBD	TBD	TBD	Cyber Security Awareness Unit Level 1	New unit	Draft new unit
Cyber Security Cross Sector Project	PwC's Skills for Australia	TBD	TBD	TBD	Cyber Security Awareness Unit Level 2	New unit	Draft new unit
Cyber Security Cross Sector Project	PwC's Skills for Australia	TBD	TBD	TBD	Network Architecture review	New unit	Draft new unit
Cyber Security Cross Sector Project	PwC's Skills for Australia	TBD	TBD	TBD	Advanced analysis and network Forensics	New unit	Draft new unit
Cyber Security Cross Sector Project	PwC's Skills for Australia	TBD	TBD	TBD	Intrusion Detection System Fundamentals	New unit	Draft new unit
Cyber Security Cross Sector Project	PwC's Skills for Australia	TBD	TBD	TBD	Advanced Intrusion Detection System concept	New unit	Draft new unit
Business Services	PwC's Skills for Australia	BSB	Business Services	BSBSMB412	Introduce cloud computing into business operations	Updated	Replace with new unit - 'Cloud Computing in Business'
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTICT814	Develop cloud computing strategies for a business	Updated	Replace with new unit - 'Cloud Computing in Business'
Business Services	PwC's Skills for Australia	BSB	Business Services	BSBRSK501	Manage Risk	Updated	Replace with new unit - 'Implementation of Risk Management'
Business Services	PwC's Skills for Australia	BSB	Business Services	BSBRSK401	Identify Risk and apply risk management processes	Updated	Replace with new unit - 'Implementation of Risk Management'
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTSAS409	Manage risks involving ICT systems and technology	Updated	Replace with new unit - 'Implementation of Risk Management'
Property Services	Artibus Innovation	CPP	Property Services	CPPSEC5005A	Implement security risk management plan	Updated	Replace with new unit - 'Implementation of Risk Management'
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTICT418	Contribute to copyright, ethics and privacy in an ICT environment	Updated	Identify unit for broader cross sector applicability

Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTNWK509	Design and implement a security perimeter for ICT networks	Updated	Identify unit for broader cross sector applicability
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTNWK511	Manage network security	Updated	Identify unit for broader cross sector applicability
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTNWK603	Plan, configure and test advanced internetwork routing solutions	Updated	Identify unit for broader cross sector applicability
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTTEN811	Evaluate and apply network security	Updated	Identify unit for broader cross sector applicability
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTNWK305	Install and manage network protocols	Updated	Identify unit for broader cross sector applicability
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTNWK403	Manage network and data integrity	Updated	Identify unit for broader cross sector applicability
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTNWK406	Install, configure and test network security Install, configure and test network security	Updated	Identify unit for broader cross sector applicability
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTNWK409	Create scripts for networking Create scripts for networking	Updated	Identify unit for broader cross sector applicability
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTNWK401	Install and manage a server	Updated	Identify unit for broader cross sector applicability
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTSAS418	Monitor and administer security of an ICT system	Updated	Identify unit for broader cross sector applicability
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTSAS505	Review and update disaster recovery and contingency plans	Updated	Identify unit for broader cross sector applicability
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTNWK601	Design and implement a security system	Updated	Identify unit for broader cross sector applicability
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTPMG601	Establish ICT project governance	Updated	Identify unit for broader cross sector applicability
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTNWK519	Design an ICT security framework	Updated	Identify unit for broader cross sector applicability

Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTNWK602	Plan, configure and test advanced server based security	Updated	Identify unit for broader cross sector applicability
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTPRG405	Automate processes	Updated	Identify unit for broader cross sector applicability
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTPRG407	Write script for software applications	Updated	Identify unit for broader cross sector applicability
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTSS00034	Basic Web Development Specialist Skill Set	Updated	Identify unit for broader cross sector applicability
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTNWK605	Design and configure secure integrated wireless systems	Updated	Identify unit for broader cross sector applicability
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTNWK607	Design and implement wireless network security	Updated	Identify unit for broader cross sector applicability
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTNWK616	Manage security, privacy and compliance of cloud service deployment	Updated	Identify unit for broader cross sector applicability
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTICT423	Select cloud storage strategies	Updated	Identify unit for broader cross sector applicability
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTPRG604	Create cloud computing services	Updated	Identify unit for broader cross sector applicability
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTNWK306	Evaluate characteristics of cloud computing solutions and services	Updated	Identify unit for broader cross sector applicability
Information and Communications Technology	PwC's Skills for Australia	ICT	Information and Communications Technology	ICTGAM404	Apply artificial intelligence in game development	Updated	Identify unit for broader cross sector applicability
Property Service	Artibus Innovation	CPP	Property Services	CPPSEC4014A	Commission and decommission networked security system	Updated	Identify unit for broader cross sector applicability
Property Service	Artibus Innovation	CPP	Property Services	CPPSEC4015A	Maintain networked security system	Updated	Identify unit for broader cross sector applicability
Property Service	Artibus Innovation	CPP	Property Services	CPPSEC4016A	Install networked security system	Updated	Identify unit for broader cross sector applicability
Property Service	Artibus Innovation	CPP	Property Services	CPPSEC4018A	Configure security devices on IT networks	Updated	Identify unit for broader cross sector applicability

Property Service	Artibus Innovation	CPP	Property Services	CPPSEC4019A	Identify and diagnose security system or network fault	Updated	Identify unit for broader cross sector applicability
Property Service	Artibus Innovation	CPP	Property Services	CPPSEC4017A	Determine security system configurations	Updated	Identify unit for broader cross sector applicability
Public Sector	SkillsIQ	PSP	Public Sector	PSPSEC006	Implement security risk treatments	Updated	Identify unit for broader cross sector applicability
Property Service	Artibus Innovation	CPP	Property Services	CPPSEC5003A	Assess security risk management options	Updated	Identify unit for broader cross sector applicability
Property Service	Artibus Innovation	CPP	Property Services	CPPSEC5004A	Prepare security risk management plan	Updated	Identify unit for broader cross sector applicability
-	-	-	Accredited Unit	VU21643	Communicate cyber security incidents within the organisation	-	Identify and potentially import into national VET system
-	-	-	Accredited Unit	VU22240	Design and implement a virtualized cyber security infrastructure for an organisation	-	Identify and potentially import into national VET system
-	-	-	Accredited Unit	VU22258	Develop a cyber security industry project	-	Identify and potentially import into national VET system
-	-	-	Accredited Unit	VU21992	Develop software skills for the cyber security practitioner	-	Identify and potentially import into national VET system
-	-	-	Accredited Unit	VU22243	Evaluate an organisation's compliance with relevant cyber security standards and law	-	Identify and potentially import into national VET system
-	-	-	Accredited Unit	VU22246	Evaluate and apply concepts and principles of cyber law	-	Identify and potentially import into national VET system
-	-	-	Accredited Unit	VU21643	Implement cyber security operations	-	Identify and potentially import into national VET system
-	-	-	Accredited Unit	VU22252	Perform basic cyber security data analysis	-	Identify and potentially import into national VET system
-	-	-	Accredited Unit	VU22245	Plan and implement a cyber security project	-	Identify and potentially import into national VET system
-	-	-	Accredited Unit	VU21990	Recognise the need for cyber security in an organisation	-	Identify and potentially import into national VET system

-	-	-	Accredited Unit	VU22250	Respond to cyber security incidents	-	Identify and potentially import into national VET system
-	-	-	Accredited Unit	VU21989	Test concepts and procedures for cyber security	-	Identify and potentially import into national VET system
-	-	-	Accredited Unit	VU21988	Utilise basic network concepts and protocols required in cyber security	-	Identify and potentially import into national VET system