Briefing Paper: Cyber Security Cross Sector Project

Prepared by PwC's Skills for Australia

About the Cyber Security Cross Sector Project

The Cyber Security Cross Sector Project, led by PwC's Skills for Australia, has reviewed the current and emerging developments in Cyber Security skills, particularly in relation to data confidentiality, protection and privacy, and identified related skills needs shared by multiple industry sectors. The objective 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. It is expected that this project will result in a significant reduction in duplication across the national vocational education and training (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, has been responsible for the direction of this cross sector project and has provided guidance, governance and made decisions based on the industry and stakeholder groups they represent. Refer to Attachment A for a list of PRG members.

Who was consulted?

PwC's Skills for Australia conducted a literature review and extensive stakeholder consultations throughout August and September 2017. Stakeholder consultation included a mix of interviews, focus groups and responses to a nationwide online survey. In total, there were 132 responses across the different consultation methods, with representation from 27 different industries and all states and territories. Refer to Attachment C for a list of stakeholders consulted.

What did we hear?

Key findings from our consultations and literature review are below. Refer to Sections 3 and 4 of the Case for Change for more information.

- High demand for workers to have better Cyber Security awareness to understand threats and risks in the digital space - that could be transferrable to any industry, occupation or level in an organisation;
- Critical shortage of Cyber Security professionals in Australia, and current Cyber Security professionals often lack the skills to respond to cyber-related security incidents and threats;
- Current gaps in Cyber Security training mean that many large employers are spending time and money to train up a Cyber Security workforce;
- Our analysis of existing units of competency suggests that there are units that could be updated to remove obsolescence, remove duplication, or improve portability.

What changes are being proposed in the Cyber Security Case for Change?

A high level summary of proposed changes is below. Refer to Section 3 of the Case for Change for more information and supporting rationale.

- Develop 2 new basic units for 'Cyber Security Awareness' (one at a nominal Certificate II level and another at nominal Certificate III level).
- 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.
- Potentially replace 6 existing Units of Competency with 2 new common units, in order to remove obsolete and/or duplicated content.
- Identify Units of Competency that already exist and could be imported into other training packages as electives to improve portability.
- Identify existing accredited units in Cyber Security to determine whether there are common units that

could be brought into the national VET system.

What does this mean for Industry Reference Committees (IRCs)?
These proposed changes, if accepted, have the potential to impact a number of training packages. Refer to Attachment B for more information.

Note that potentially materially impacted IRCs are requested to indicate approval and support for the proposed changes prior to submission of the final Case for Change to the AISC.

The ask of your IRC is to indicate approval and support for the Cyber Security Case for Change via this link: https://pwc.to/2yi1EHk, ideally by no later than 15 November 2017.

At a Case for Change stage, any IRC that does indicate its approval and support is doing so on the understanding that these are proposed changes only, and further consultation will be undertaken in if the Case for Change proceeds to a second phase of work. Ultimately, it will be the home IRC's decision whether to adopt any proposed changes that involve existing units in the IRCs training package. We would appreciate each IRC endeavouring to **please indicate a response by 15 November 2017**.

Approve and support the Cyber Security Case for Change

For queries contact info@skillsforaustralia.com