Australian Industry and Skills Committee

DEFENCE ELECTRONIC FORENSICS

Case for Change

Name of allocated IRC: Public Safety
Name of the SSO: Australian Industry Standards

1. Administrative information

*For a list of the products proposed to be reviewed as part of this project, please see **Attachment A**.*

Name of IRC(s):	Public Safety
Name of SSO:	Australian Industry Standards

1.1 Name and code of Training Package(s) examined to determine change is required

DEF Defence Training Package

2. The Case for Change

*For information on the job roles to be supported through the proposed qualifications updates, enrolments data, completion rates, and the number of RTOs delivering these qualifications please see **Attachment B**.*

2.1 Rationale for change

Defence electronic forensics (sometimes known as digital forensics) is a branch of forensic science encompassing recovery and investigation of material found on digital devices, often in relation to computer crime.

There have been significant advancements in technology where forensic investigators are dealing with evidence gathering from more complex devices and systems. The software tools used in forensics are often updated therefore Defence personnel need to keep pace with these changes to be able to use modern devices and to analyse cloud storage systems. The collection, handling, and preservation of evidence during a workplace investigation is critical as digital evidence is now used to prosecute all types of crimes, not just e-crime. It is therefore essential that Defence forensics personnel are fully equipped with the latest skills and knowledge as it can impact on the outcome of an investigation.

Defence seeks to undertake a review of the Cert IV and Diploma in Electronic Forensics including the review of 12 Units of Competency as part of this Case for Change. The qualifications provide individuals with the ability to apply a range of integrated technical and theoretical concepts in electronic forensics.

Implications of not implementing changes in relation to electronic forensics in a Defence environment include:

- A missed opportunity to achieving more successful electronic forensic investigation outcomes
- Difficulties in meeting Defence and industry operating standards
- Delays in developing new Defence procedures
- Increased operating costs based on inefficiencies
- Difficulties meeting required Defence quality standards

The products in the nominated qualification were last reviewed in 2015.

2.2 Evidence for change

Defence draws on its commitment to the Australian Defence Force Strategic Plan contained in the Defence White Paper to 2030. This strategy seeks to increase the capacity and capability of its staff – this includes growing the integrated Defence workforce. Attracting and retaining the future Defence workforce will be a major challenge in the future.

As a result, Defence continues to invest and respond to the development of programs aimed at advancing workforce skills. This is achieved through the delivery of high-quality training in a range of fields including, leadership, and management in a wide variety of fields, including cyber security, intelligence, forensics, health, security analysis and engineering.

Defence have reviewed post training implementation feedback data which is used to address areas in a program that have changed and/or that are inconsistent with the standards. Defence recommended that the Cert IV and Diploma Electronic Forensics be reviewed as a routine project.

2.3 Consideration of existing products

This project proposes to review existing Defence and imported units of competency only and not the creation of new products.

2.4 Approach to streamlining and rationalisation of the training products being reviewed

There are no Defence products identified at this stage for deletion however Defence systematically reviews the viability and relevance of Training Package products and removes them based on their capability needs.

3. Stakeholder consultation

3.1 Stakeholder consultation undertaken in the development of Case for Change

*For a full list of industry-specific stakeholders that actively participated in the stakeholder consultation process undertaken to develop the Case for Change, please see **Attachment C**.*

Defence followed its own rigorous and highly structured communications strategy when undertaking the engagement process for this Case for Change. Defence consulted stakeholders from sections across its three services (Army, Navy and Airforce) and across multiple jurisdictions.

Department section Learning Leads of the relevant qualifications were consulted as part of this process who in turn have the delegation of authority to approve development changes on behalf of their sections. Feedback was coordinated centrally through the Defence Education, Learning and Training Authority (DELTA) and then communicated to AIS.

3.2 Evidence of Industry Support

*For a list of the issues raised by stakeholders during consultation and the IRC's response to these, please see **Attachment D.***

Defence Education, Learning and Training Authority (DELTA) coordinate Defence Training Package product changes through their own structured consultation process. Heads of sections and Learning Leads in the three Defence service areas of Army, Airforce and Navy are responsible for identifying Training Package issues and proposing reviews and updates to qualifications and skills standards so that they are consistent with industry practice and meet Defence capability requirements.

Defence legal Learning Leads have determined that, based on changes in electronic forensics technology including software tools, Defence forensics experts will need to update to keep pace with the recent updates and changes to digital devices and storage systems.

Please see attachment D.

3.3 Proposed stakeholder consultation strategy for project

*Note: For a full list of industry-specific stakeholders who are planned to be contacted to participate in the stakeholder consultation process undertaken for this project, please see **Attachment E**.*

Key Industry stakeholders have been identified in consultation with Defence and the Public Safety IRC.

AIS maintains a comprehensive database of industry contacts and stakeholders who receive targeted communications related to consultation on industry skills and training package development projects.

In addition, Defence-specific stakeholders in any consultation process are documented as per Defence security protocols sighting the Defence section areas only and not identifying names.

Standard online/video consultation, email correspondence and promotional activity are conducted via targeted communications including approved social media methods.

A recently developed **Engagement Hub** on the AIS website provides a one stop portal for information about how all stakeholders can participate and inform Training Package development work.

AIS, on behalf of the Public Safety IRC, will promote the opportunity to contribute through the AIS website, EDM's, AIS newsletter and public notifications. Stakeholders will also be notified of key milestones throughout the life of the project, including requests for feedback on draft materials. Stakeholder engagement and consultation will occur over the life of the project via a combination of the following methods:

- Direct engagement: Face to face consultations, Site visits, Phone, emails, video/teleconferencing meetings
- Industry forums and conferences
- Webinars
- Online feedback mechanisms
- STA direct engagement

Participation in Defence projects is achieved centrally through the Defence Education, Learning and Training Authority (DELTA). Branch owners in each of the three Defence Services, Army, Navy and Airforce, are responsible for their relevant qualifications and are consulted as part of this process through DELTA which includes regional and remote centres.

4. Licencing or regulatory linkages

Defence does not require State based licences; however, it does comply with national regulatory and licensing requirements where they apply. There are no licensing or regulatory requirements attached to these qualifications.

5. Project implementation

5.1 Prioritisation category

This Case for Change proposes that this review be progressed as a routine project.

In accordance with the AISC Training Package Prioritisation Report and to coordinate the release of updated products, the Public Safety IRC recommends a routine update and implementation of this project.

5.2 Project milestones

Key project milestones include:

- AISC project approval – June 2021
- Draft 1 consultation – November 2021
- Stakeholder validation – –March 2022
- Quality Assurance – April/May 2022
- Final consultation with states and territories – June 2022
- CfE submitted for approval – 30 June 2022.

5.3 Delivery or implementation issues

Training implementation evaluation is conducted routinely by Defence and is considered an essential part of training and assessment cycle to be able to reflect, analyse, and improve its effectiveness and efficiency. Aspects raised by Defence and/ or stakeholders are included as part of the Training Package review.

Appropriate and relevant advice and suggestions will be provided in the Companion Volume Implementation Guide in addition to links to relevant resources.

6. Implementing the Skills Minister's Priority reforms for Training Packages (2015 and October 2020)

Training delivery information will be provided within the supporting Companion Volume Implementation Guide. This guide exists to provides clear and useful information. It also includes clear guidance on the context of the range of job role environment applications in appendix form and has useful advice for implementers and educators.

Supporting individuals to move more easily between related occupations is managed centrally by Defence in the defence context. Pathway information is not explicitly provided in the CVIG for security reasons however there is information in the CVIG to support the following:

- Access and equity are described and addressed with advice on reasonable adjustment for learners
- Foundation skills is identified and described against the Australian Core Skills Framework (ACSF) and skill cluster known as the foundation skills for work framework.

The current products may be suitable for use by multiple industry sectors and will provide improved opportunities for individuals operating in relevant sectors to transfer acquired skills and knowledge into multiple sectors and/or operating environments.

Greater recognition of skill sets and work with industry to support their implementation: This Case for Change proposes the review of qualification(s)however Defence actively look to add appropriate Skill Sets to support the skills capability of their staff.

This Case for Change was agreed to by the Public Safety IRC

Name of Chair	Mark Burgess
Signature of Chair	m A Burgess
Date	14 May 2021

Attachment A: Training Package components to change

SSO: Australian Industry Standards Limited

Contact details: David Dixon - Chief Operating Officer

Date submitted: 14 May 2021

Project number	Project Name	Qualification/ Unit / Skillset	Code	Title	Details of last review *(endorsement date, nature of this update transition, review, establishment)*	Change Required
1	Defence Electronic Forensics	Qualification	DEF43115Y	Certificate IV in Electronic Forensics	22/Oct/2015 - Establishment	Update
1	Defence Electronic Forensics	Qualification	DEF53115Y	Diploma of Electronic Forensics	22/Oct/2015 - Establishment	Update
1	Defence Electronic Forensics	Unit	DEFFOR001Y	Inspect, maintain and test electronic forensic equipment	17/Aug/2017 - Transition	Update
1	Defence Electronic Forensics	Unit	DEFFOR002Y	Conduct initial electronic investigation	22/Oct/2015- Establishment	Update
1	Defence Electronic Forensics	Unit	DEFFOR003Y	Gather and analyse electronic information	22/Oct/2015 - Establishment	Update
1	Defence Electronic Forensics	Unit	DEFFOR004Y	Capture forensic photographic images	22/Oct/2015 - Establishment	Update

1	Defence Electronic Forensics	Unit	DEFFOR005Y	Compile and submit electronic media forensic documentation	22/Oct/2015 - Establishment	Update
1	Defence Electronic Forensics	Unit	DEFFOR006Y	Conduct electronic data search and analysis	22/Oct/2015 - Establishment	Update
1	Defence Electronic Forensics	Unit	DEFFOR007Y	Set up, operate and maintain a portable audio recorder	22/Oct/2015 - Establishment	Update
1	Defence Electronic Forensics	Unit	DEFFOR008Y	Detect, record and collect electronic evidence	22/Oct/2015 - Establishment	Update
1	Defence Electronic Forensics	Unit	DEFFOR009Y	Give evidence of electronic media crime	22/Oct/2015 - Establishment	Update
1	Defence Electronic Forensics	Unit	DEFFOR010Y	Produce an electronic media image for forensic purposes	22/Oct/2015 - Establishment	Update
1	Defence Electronic Forensics	Unit	DEFFOR011Y	Assess, control and examine electronic incident scenes	22/Oct/2015 - Establishment	Update
1	Defence Electronic Forensics	Unit	DEFGEN023Y	Capture video images	22/Oct/2015 - Transition	Update

Attachment B: Job role, enrolment information, the number of RTOs currently delivering these qualifications

Please set out the job roles to be supported through the updated qualifications, enrolment data over the past three years in which data is available for each qualification, completion rates for each qualification, and the number of RTOs delivering these qualifications.

Note: Defence AVETMIS statistics are not made public and not available in this Case for Change.

Job role	Qualification to be updated to support the job role	Enrolment data (for the past three years)	Completion rates (for the past three years)	Number of RTOs delivering (for the past three years)
441- Defence Force Members, Fire Fighters and Police	DEF43115Y Certificate IV in Electronic Forensics	Not reported	Not reported	1
441- Defence Force Members, Fire Fighters and Police	DEF53115Y Diploma of Electronic Forensics	Not reported	Not reported	1
	DEFFOR001Y Inspect, maintain and test electronic forensic equipment	Not reported	Not reported	1
	DEFFOR002Y Conduct initial electronic investigation	Not reported	Not reported	1
	DEFFOR003Y Gather and analyse electronic information	Not reported	Not reported	1
	DEFFOR004Y Capture forensic photographic images	Not reported	Not reported	1
	DEFFOR005Y Compile and submit electronic media forensic documentation	Not reported	Not reported	4

	DEFFOR006Y Conduct electronic data search and analysis	Not reported	Not reported	1
	DEFFOR007Y Set up, operate and maintain a portable audio recorder	Not reported	Not reported	1
	DEFFOR008Y Detect, record and collect electronic evidence	Not reported	Not reported	1
	DEFFOR009Y Give evidence of electronic media crime	Not reported	Not reported	1
	DEFFOR010Y Produce an electronic media image for forensic purposes	Not reported	Not reported	1

Attachment C: List of stakeholders that actively participated in the consultation process of the Case for Change

Name of stakeholder	Title	Organisation	Organisation type (e.g. Employer, peak body, union, RTO, regulator)	Jurisdiction/town/city (e.g. NSW/Sydney)
Branch owners and Leads of Subject	N/A	Defence	Military	National
Defence Education, Learning and Training Authority (DELTA)	NA	Australian Defence College Canberra	Military	National
State Training Authorities	N/A	All State and Territory training authorities	State Training Authority	States

Attachment D: Issues Raised by Stakeholders during consultation on the development of the Case for Change

Stakeholder Type	Issues Raised	IRC's Response to Issues Raised
Victorian State Training Authority	The qualifications have not been updated since 2015 and the proposed changes relate to the significant advances in technology and increasing number and complexity of modern devices available since that time. There have been significant updates to the BSB and ICT Training Packages, and it is timely to update these units of competency that are a feature of the Defence Forensics qualifications. Cyber Security is also mentioned in the CFC and new products are available in the ICT Training Package that may have useful application within Defence Forensics.	The feedback items related to updating imported units in addition to Cyber Security are present in the Case for Change and will be incorporated into the project if approved.

Attachment E: List of stakeholders to be contacted as part of the development of the Case for Endorsement

Name of stakeholder	Title	Organisation	Organisation type (e.g. Employer, peak body, union, RTO, regulator)	Jurisdiction/town/city (e.g. NSW/Sydney)
Branch owners and Defence Leads of Subject	N/A	Defence	Military	National
Defence Education, Learning and Training Authority (DELTA)	NA	Australian Defence College Canberra	Military	National
State Training Authorities	N/A	State and Territory training authorities	State Training Authority	States
ASQA	N/A	Australian Skills Quality Authority	National Regulator	National
Public Safety Industry Reference Committee	N/A	Department of Defence representative	Military Employer/RTO	National

The Case for Endorsement development will also involve contacting stakeholders from the following organisational types across all states and territories within Australia as required:

- Industry Reference Committee (IRC) Representatives
- Employers (Non-IRC)
- Peak Industry Bodies
- Unions
- Other regulators as relevant
- RTOs
- Other/Consultants