EXPLANATORY STATEMENT

Issued by authority of the Minister for Home Affairs

AusCheck Act 2007

AusCheck Legislation Amendment (Critical Infrastructure Background Check) Regulations 2023

The *AusCheck Act 2007* (AusCheck Act) provides authority for the conduct and coordination of background checks under the AusCheck scheme as established by the *AusCheck Regulations 2017* (AusCheck Regulations). The purpose of the AusCheck Act is to provide a framework for coordinating and conducting background checks of an individual's criminal, security and other background checking, and for related purposes.

The AusCheck Act was amended on 2 April 2022 by Schedule 1 to the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* to extend the AusCheck scheme to enable background checking of an individual if a responsible entity for a critical infrastructure asset, within the meaning of those terms given by the *Security of Critical Infrastructure Act 2018* (SOCI Act), has a critical infrastructure risk management program (CIRMP) that permits a background check to be conducted under the AusCheck scheme.

A responsible entity is required to establish, maintain and comply with a CIRMP under Part 2A of the SOCI Act if the asset is specified in rules made under section 30AB of that Act. The Minister for Home Affairs has recently released proposed rules for consultation, to specify assets under section 30AB that are the following types of assets as defined by the SOCI Act: a critical broadcasting asset, critical domain name system, critical data storage or processing asset, critical electricity asset, critical energy market operator asset, critical gas asset, certain critical hospital, critical food and grocery asset, critical freight infrastructure asset, critical freight services asset, critical liquid fuels asset, payment system and critical water asset (draft CIRMP Rules).[1] Separately, the Minister for Home Affairs has also released proposed rules for consultation specifying that Osborne Naval Shipyard is a critical infrastructure asset to which Part 2A also applies (draft Naval Shipbuilding Rules).[2]

Legislative authority

Paragraph 8(1)(ba) of the AusCheck Act has the effect that the AusCheck Regulations may provide for the expansion of the AusCheck scheme relating to the conduct and coordination of background checks of an individual if a CIRMP permits a background check to be conducted under the AusCheck scheme.

Under section 30AH of the SOCI Act, a CIRMP is a written document that relevantly complies with such requirements (if any) specified for paragraph (1)(c). Subsection 30AH(4) provides that rules specified for paragraph (1)(c) may require that a CIRMP include one or more provisions that permit a background check to be conducted under the AusCheck scheme.

[1] Publically available via: Engagement on critical infrastructure reforms (homeaffairs.gov.au)

[2] Publically available via: Osborne Naval Shipyard Formal Consultation (auscheck.gov.au)

Under the proposed rules to be made under sections 30AB and 30AH of the SOCI Act, the responsible entities will relevantly need to:

- under the draft CIRMP Rules—establish a process or system in their CIRMP to assess, on an ongoing basis, the suitability of a 'critical worker' to have access to the 'critical components' of their asset(s) which could include the conduct of background checks under the AusCheck scheme, and
- under the draft Naval Shipbuilding Rules—require a background check to be conducted for an individual who has unescorted access to Osborne Naval Shipyard.

This provides legislative authority for a background check to be conducted under the AusCheck scheme where a CIRMP permits such a check to be conducted as required or permitted by the proposed rules.

The AusCheck Regulations establish the AusCheck scheme, which relates to the conduct and coordination of background checks by AusCheck, a background checking function of the Department of Home Affairs, for the purposes of the *Aviation Transport Security Act 2004*, the *Maritime Transport and Offshore Security Act 2003*, where permitted by a CIRMP, in connection with a major national event, or where any other Act that expressly requires or permits a background check to be conducted under the AusCheck scheme, such as the *National Health Security Act 2007*. The AusCheck Regulations prescribe a range of matters for the operation of the AusCheck scheme.

Purpose

The purpose of the *AusCheck Legislation Amendment (Critical Infrastructure Background Check) Regulations 2023* (Amendment Regulations) is to amend the AusCheck Regulations to provide for the establishment and operation of the AusCheck background checking scheme for an individual for whom a CIRMP permits a background check.

The measures inserted into the AusCheck Regulations by Schedule 1 include:

- introducing an ability for AusCheck to undertake a background check of an individual if such a check is permitted under a CIRMP (a critical infrastructure background check), and to conduct a further background check if the information provided for an initial background check was incomplete or the application requirements were not met;
- specifying the information required to be included in an application for a critical infrastructure background check;
- defining terms for the purposes of a critical infrastructure background check;
- providing advice about the outcome of a critical infrastructure background check to the individual and the responsible entity,
- requirements for conducting electronic and in-person identity verification;
- authorising the Secretary to grant an exemption from specified requirements of an electronic or in-person identity verification check if the individual is unable to meet those requirements;
- requiring the Secretary to give the individual written notice of, and reasons for, a preliminary assessment that an individual has an unfavourable criminal history and enable the individual to make representations;
- authorising the Secretary to request an individual or responsible entity do a specified

thing to ensure information is provided and application requirements are met, and to cancel a background check where that request is not complied with;

- requiring the Secretary to give further advice about a critical infrastructure background check if the Secretary becomes aware that the initial advice is inaccurate or incomplete;
- imposing an obligation on a responsible entity to inform the Secretary of certain decisions made in relation to granting access to the critical infrastructure asset or the revocation of access to the critical infrastructure asset, and create offences for failure to satisfy those obligations;
- authorising applications to be made to the Administrative Appeals Tribunal for review of decisions of the Secretary to refuse to grant an exemption in relation to identity verification requirements or to advise that an individual has an unfavourable criminal history,
- authorising the Secretary to charge a fee for an application for an critical infrastructure background check, and
- setting out offences that are CIRMP-security-relevant offences in Schedule 2.

Impact and effect

The impact of the Amendment Regulations is to provide for the extension of the AusCheck scheme to background checking of an individual for whom a CIRMP permits a background check. This is intended to have a positive impact on the management of personnel security risks for critical infrastructure assets by providing responsible entities with the option of accessing the AusCheck scheme. It is not anticipated that there will be any adverse impact or effect from the making of the Amendment Regulations.

Consultation

AusCheck developed the policy rationale implemented by the Amendment Regulations in consultation with the Department of Defence, who will be the responsible regulator for naval shipbuilding assets under the draft Naval Shipbuilding Rules.

The policy being implemented by the Amendment Regulations was also made available for public consideration and comment during the course of consultation on the draft CIRMP Rules.

The Minister for Home Affairs commenced a 45 day consultation period on 5 October 2022 and concluded consultation on 18 November 2022. The consultation was advertised on the Department's website and notice of the consultation was emailed to 2619 stakeholders, inviting written submissions. The following occurred during the period;

- Two public virtual town halls on 10 October and 12 October 2022 (257 and 297 attendees, respectively);
- Four question & answer sessions (Q&A sessions) on 13 October, 18 October, 25 October and 1 November 2022 (101, 141, 162 and 101 attendees, respectively);
- Ten bilateral meetings at the request of individual stakeholders, and
- Twenty email responses to queries.

The Department ultimately received 37 written submissions.

Stakeholder feedback included concerns regarding workers' privacy and the right to work, issues which have been considered in the Statement of Compatibility with Human Rights at Attachment B.

Much of the stakeholder feedback consisted of clarification on the operation of the policy. The Department has published a draft Risk Management Program Guidance document on the website which has a section on the AusCheck scheme to draw out aspects of the scheme in further detail. Additionally, the Department has created an FAQ document based on queries received throughout the consultation period, including on the AusCheck scheme, and this has also been made publically available on the Department's website. The Department is willing to produce more guidance and undertake further engagement and education on this aspect of the CIRMP, if required.

Regulatory impact statement

The then Office of Best Practice Regulation, now Office of Impact Analysis, was consulted prior to making the Amendment Regulations, and advised that a regulatory impact statement was not required (OBPR ID: 44773).

Status and commencement

The Amendment Regulations is a legislative instrument for the purposes of the *Legislation Act 2003*.

The Amendment Regulations are compatible with human rights and freedoms for the purposes of the *Human Rights (Parliamentary Scrutiny) Act 2011*. The statement of compatibility with human rights is included at Attachment B.

The Amendment Regulations commence on the day after registration.

ATTACHMENT A

Details on provisions

AusCheck Legislation Amendment (Critical Infrastructure Background Check) Regulations 2023

Section 1 – Name

Section 1 provides that the name of the regulations is the *AusCheck Legislation Amendment (Critical Infrastructure Background Check) Regulations 2023* (Amendment Regulations).

Section 2 – Commencement

Section 2 provides for the commencement of the Amendment Regulations, occurring the day after registration on the Federal Register of Legislation.

The commencement of the Amendment Regulations at the first available opportunity after they are made provides for the framework and mechanism for critical infrastructure background checking to be in place for background checks to be conducted as soon as a responsible entity's critical infrastructure risk management program, that permits a background check to be conducted under the AusCheck scheme, is in force. This will provide critical infrastructure sectors with certainty, and will allow processes and systems to be developed and enshrined in their risk management programs.

Section 3 – Authority

Section 3 prescribes that the Amendment Regulations are made under the *AusCheck Act 2007* (AusCheck Act).

Subsection 18(1) of the AusCheck Act provides that the Governor-General may make regulations prescribing matters required or permitted by the AusCheck Act to be prescribed, or necessary or convenient to be prescribed for carrying out or giving effect to the AusCheck Act. Paragraph 8(1)(ba) of the AusCheck Act provides a broad discretion for the making of regulations with respect to the conduct of background checks in relation to particular individuals under the AusCheck scheme.

Relevantly, the AusCheck Act provides that:

- the regulations may provide for the establishment of the AusCheck scheme relating to the conduct and coordination of background checks of individuals if the check is of an individual in relation to a critical infrastructure risk management program that permits a background check of an individual to be conducted under the AusCheck scheme (paragraph 8(1)(ba));

- the AusCheck scheme may empower the Secretary to give directions to an applicant for a background check, or to a person who is required to take action relating to matters connected with a background check (subsection 11(1)), and

- the regulations may provide for the imposition of penalties, not exceeding 100 penalty units, for a contravention of the regulations (paragraph 18(2)(c)).

The amendments being made by the Amendment Regulations to the AusCheck Regulations by Schedule 1 are supported by the abovementioned provisions of the AusCheck Act.

Section 4 – Schedules

Section 4 provides that each instrument specified in a schedule to this instrument would be amended or repealed as set out in this instrument and any other item in a schedule to this instrument has effect according to its terms. There is one Schedule to the Amendment Regulations.

Schedule 1—Amendments

Part 1—Critical Infrastructure background check

AusCheck Regulations 2017

Schedule 1 to the Amendment Regulations amends the AusCheck Regulations to extend the AusCheck scheme to apply to background checks of an individual in connection with the requirements of responsible entity's critical infrastructure risk management program, these background checks are described as 'critical infrastructure background checks'.

Item 1– Section 4 (after paragraph (b) of the note to the heading)

Item 1 inserts new paragraph (ba) in the note following the heading of section 4 of the AusCheck Regulations, which makes reference to terms defined in section 4 of the AusCheck Act that are used in various places in the AusCheck Regulations.

Paragraph (ba) make references to the definition of 'critical infrastructure risk management program' that was recently inserted into the AusCheck Act by the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022*. That Act provided for the extension of the AusCheck scheme to a critical infrastructure risk management program that permits a background check of an individual to be conducted under the AusCheck scheme, and inserted the regulation-making powers into the Act upon which the proposed Regulations rely.

A *critical infrastructure risk management program* is defined by section 4 of the AusCheck Act to have the same meaning as in the *Security of Critical Infrastructure Act 2018*.

Critical infrastructure risk management program is defined in section 30AH of the *Security of Critical Infrastructure Act 2018*.

Item 2 — Section 4 (paragraph (c) of the definitions of Category A identification document, Category B identification document and Category C identification document)

Item 2 amends paragraph (c) of the definitions of *Category A identification document, Category B identification document,* and *Category C identification document* to extend the application of those paragraphs to an individual for whom a *critical infrastructure risk management program* (or CIRMP, see Item 4) permits a background check.

Paragraph (c) of each definition previously applied only in relation to a major national event (MNE) accreditation. For the avoidance of doubt, paragraph (c) of each definition does not apply in relation to applications for background checks conducted and coordinated by AusCheck in relation to aviation and maritime security cards, or for access to security sensitive biological agents.

The amendments to paragraph (c) of definitions of *Category A identification document, Category B identification document,* and *Category C identification document* adopt a standard of proof consistent with the *National Identity Proofing Guidelines* published by the Commonwealth of Australia in 2016 (National Identity Proofing Guidelines).

The amendments made by Item 2 will mean that the identification requirements for an individual for whom a CIRMP permits a background check, will be the same as the identification requirements for MNE.

Category A identification document

The amendment made by Item 2 to paragraph (c) of this definition has the effect that for an individual for whom a CIRMP permits a background check, a *Category A identification document* means:

- for an individual who was born in Australia and is an Australian citizen—either the individual's Australian birth certificate or a notice given to the individual under section 37 of the *Australian Citizenship Act 2007*(subparagraph (c)(i)), or

- for any other individual—a valid document that provides evidence of the start of the individual's identity in Australia (subparagraph (c)(ii)).

A Category A identification document must be 'valid' because it is possible for a document to become invalidated after it is produced, for example by cancellation or by subsequent replacement. A replacement document may be issued if the person changes their name or registered sex on their birth certificate, or if the original document is lost, damaged, or stolen.

Category B identification document

The amendment made by Item 2 to paragraph (c) of this definition has the effect that for an individual for whom a CIRMP permits a background check, a document is a *Category B identification document* when it is a current and valid document that:

- is issued to the individual by a Commonwealth, State or Territory Department or agency, or by a government of a foreign country or an agency of a government of a foreign country (subparagraph (c)(i)),
- provides photographic proof of the individual's identity (subparagraph (c)(ii)), and
- includes the individual's signature (subparagraph(c)(iii)).

For paragraph (c) of this definition, a Category B identification document must be 'current' because this type of document is typically issued for a specified period of time and has an expiry date after which the document ceases to be current. For example, an unrestricted driver licence issued by a State or Territory or an Australian passport may be issued for a period of 10 years. After the expiration date specified on the licence or in the passport, it ceases to be a 'current' Category B identification document.

A Category B identification document for paragraph (c) of this definition must also be 'valid' because it is possible for a document to become invalidated after it is produced, for example by cancellation or by subsequent replacement if the document is lost, damaged, or stolen.

The guiding note following paragraph (c) of this definition refers to a current and valid Australian or foreign passport or a driver licence as an example of a Category B identification document. In this example, a Category B identification document would be a licence or passport that has not reached the expiry date and has not been superseded by a replacement document.

Category C identification document

The amendment made by Item 2 to paragraph (c) of this definition has the effect that for an individual for whom a CIRMP permits a background check, a document is a *Category C identification document* when it is a current and valid document that provides evidence of the individual's use of identity while operating in the community (including a community outside of Australia).

The guiding note following paragraph (c) of this definition refers to a current and valid Medicare card, or a bank or credit card issued by a bank as an example of a Category C identification document.

As mentioned above in relation to a Category B identification document, a Category C identification document must be 'current' because a document of this type is typically issued for a period of time and has an expiry date after which the document will cease to be current.

Similarly, a Category C identification document must be 'valid' because it is possible for a document to become invalidated after it is produced. For example, a person may have lost their Medicare card and requested a new one. The Department of Human Services would cancel that card and issue a replacement card with a new expiry date. If the individual located their 'lost' Medicare card, it would appear to be 'current' as the expiry date had not passed but it would not be 'valid' as that card would have been cancelled by the Department of Human Services.

Item 3 – Section 4 (Category D identification document)

Item 3 amends the definition of Category D identification document to extend the application of the requirement to provide a Category D identification document to an individual for whom a CIRMP permits a background check. For the avoidance of doubt, a Category D identification document does not apply in relation to applications for background checks relating to aviation and maritime security cards, or for access to security sensitive biological agents.

In effect, this amendment provides that for an individual for whom a CIRMP permits a background check, a document is a Category D identification document under paragraph (d) for the purposes of a critical infrastructure trusted insider assessment when it is a valid document that:

- provides evidence of the individual's current residential address (which may be a residential address outside of Australia) (paragraph (a)), and
- is less than 6 months old (paragraph (b)).

As noted above at Item 2 in relation to Category A, B and C identification documents, a Category D identification document must be 'valid' at the time it is used to support an application for a background check because it is possible for a document to become invalidated after it is produced.

The guiding note following this definition mentions a current utilities notice as an example of a Category D identification document. An illustration of the details of the document becoming invalidated would be where the individual has changed their residential address or cancels their account with the named utility service provider after that utilities notice has been issued.

Other examples of a Category D identification document include a bank statement, electoral roll registration or motor vehicle registration.

Item 4 –Section 4

Item 4 inserts further additional definitions into section 4 of the AusCheck Regulations.

CIRMP

This definition provides that *CIRMP* is short for critical infrastructure risk management program.

As noted above at Item 1, *critical infrastructure risk management program* is defined by section 4 of the AusCheck Act to have the same meaning as in the *Security of Critical Infrastructure Act 2018* (SOCI Act).The term critical infrastructure risk management program is defined in section 5 of the SOCI Act to have the meaning given in section 30AH of that Act.

Under section 30AH of the SOCI Act, a critical infrastructure risk management program is a written program that a responsible entity for a critical infrastructure asset must establish to:

- identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset
- as far as reasonably practicable—minimise or eliminate any material risk of such a hazard occurring, and
- as far as reasonably practicable—mitigate the relevant impact (as defined by section 8G of the SOCI Act) of such a hazard on the asset.

The purpose of a critical infrastructure risk management program is to ensure responsible entities have a comprehensive understanding of the threat environment in relation to its asset, and develop processes and procedures to effectively manage a range of hazards – including personnel hazards – having a direct or indirect impact on the availability, reliability and integrity of, or confidentiality of information held by or about, their critical infrastructure asset(s).

'Personnel hazards' in this context include employees exploiting their legitimate access to critical infrastructure assets for unauthorised purposes including criminal activity, corporate espionage, sabotage and foreign interference. A critical infrastructure background check is an option that is available to assist a responsible entity in its identification and management of personnel hazards, in accordance with the processes and systems established in its critical infrastructure risk management program.

CIRMP criminal record

This definition provides that an individual has a *CIRMP criminal record* if the individual has been:

- convicted of a *CIRMP level 1 offence* (paragraph (a)), or

- convicted of a *CIRMP level 2 offence* and sentenced to any term of imprisonment for the offence(paragraph (b)).

The term *conviction* is defined in section 4 of the AusCheck Regulations, and is amended by Item 5, below.

The purpose of including this definition in the Amendment Regulations is to provide a short-hand reference by which the defined concept is captured in the ability of AusCheck to conduct a background check in relation to an individual for whom a CIRMP permits a background check (under section 11AD(1)(a), as would be inserted by Item 20).

CIRMP level 1 offence

This definition provides that *CIRMP level 1 offence* means a *CIRMP-security-relevant offence* mentioned in an item in the table in Item 1 of Schedule 2.

The purpose and effect of including this definition in the Amendment Regulations is to provide a short-hand reference for the concept.

CIRMP level 2 offence

This definition provides that *CIRMP level 2 offence* means a *CIRMP-security-relevant offence* mentioned in an item in the table in Item 2 of Schedule 2.

The purpose and effect of including this definition in the Amendment Regulations is to provide a short-hand reference for the concept.

CIRMP-security-relevant offence

This definition provides that *CIRMP-security-relevant offence* means an offence mentioned in an item in a table in Schedule 2 against a law of the Commonwealth, a State or a Territory.

The purpose and effect of including this definition in the Amendment Regulations is to provide a short-hand reference for the concept.

Item 5 – Section 4

Item 5 amends the definition of *conviction* to insert a reference to a critical infrastructure background check. This amendment is connected to the inclusion of the definition of *CIRMP criminal record*, outlined above.

Item 6 – Section 4

Item 6 inserts a definition in section 4 of *critical infrastructure asset.*

Critical infrastructure asset is defined as having the same meaning as in the SOCI Act.

Section 5 of the SOCI Act provides that *critical infrastructure asset* has the meaning given by section 9 of that Act. Section 9 lists the types of critical assets that are *critical infrastructure assets* for the purposes of the SOCI Act.

The purpose and effect of the amendment made by Item 6 is to adopt the meaning given to this term by the SOCI Act in the AusCheck Regulations.

Item 7 – Section 4 (*paragraph (d) of the definition of identification document*)

Item 7 amends paragraph (d) of the definition of *identification document* to insert a reference to an individual for whom a CIRMP permits a background check.

This amendment is connected to the amendments made to the definitions of Category A identification document, Category B identification document, Category C identification document and Category D identification document outlined above, and to the amendment made by Item 9 below to the definition of *verifying person*.

Item 8 – Section 4

This Item inserts a definition of *responsible entity*.

This definition provides that *responsible entity* has the same meaning as in section 12L of the SOCI Act. Section 12L of the SOCI Act describes the circumstances in which an entity is the responsible entity for a specified type of *critical infrastructure asset*.

The purpose and effect of the amendment made by Item 8 is to adopt the meaning given to this term by the SOCI Act in the AusCheck Regulations.

Item 9 – Section 4 *(definition of verifying person)*

Item 9 repeals and substitutes a new definition of *verifying person* to extend the previous definition, which dealt with who was a *verifying person* for the purposes of accreditation for a major national event, to include a reference to an individual for whom a CIRMP permits a background check.

The definition now operates to provide that *verifying person*, for an identity verification check of an individual, means:

- if the identity verification check is in connection with MNE accreditation in relation to a major national event:
    - AusCheck (subparagraph (a)(i)), or
    - the organising body for the major national event(subparagraph (a)(ii)), or
    - a person acting on behalf of AusCheck or the organising body (subparagraph (a)(iii)), or

- if the identity verification check is permitted under a CIRMP:
    - AusCheck (subparagraph (b)(i)), or
    - the responsible entity in relation to whom the CIRMP applies (subparagraph (b)(ii)), or
    - a person acting on behalf of AusCheck or the responsible entity (subparagraph (b)(iii)).

Subparagraphs (b)(ii) and (iii) of the definition are required to allow either AusCheck or a responsible entity to authorise another person to complete an identity check on their behalf. This is particularly important in relation to the conduct of in-person identity verification under new section 21W (see Item 24). This would provide, for example, for an applicant for a *critical infrastructure background check* to present to a post office to complete an in person identity verification on behalf of a responsible entity.

The effect of this amendment is that the definition will specify who is a *verifying person* for an identity verification check in circumstances where an identity verification check is permitted under a CIRMP. Identity verification is an essential component of a critical infrastructure background check under Subdivision A of Division 5B of Part 2 of the AusCheck Regulations (introduced by Item 24).

Items 10 – 14 Subsection 5(1)

Items 10 to 14 amend subsection 5(1) which deals with 'required information' that must be provided to AusCheck when applying for a background check by an individual or the responsible entity that makes an application for a background check on the individual's behalf. Subsection 5(1) prescribes, among other things, identifying information, residential address information, the name and business address of the employer or education institution, and relevant details about the work the person is or will be performing. Pertinent information would be disclosed by AusCheck to background checking partner agencies (e.g. to ASIO for security assessments, to ACIC for criminal history assessments, to 'the Immigration Department' for immigration status and work entitlement assessments) so that relevant checks can be made in relation to the individual.

Appropriate safeguards on personal information collected under these measures are provided for through the *Privacy Act 1988* (Privacy Act) that requires that all personal information collected and held by the Government must adhere to the Australian Privacy Principles (APPs) as set out under the Privacy Act. As an APP entity, failure to comply with privacy obligations can have serious legal, financial and reputational consequences for the Department of Home Affairs (the Department).

The Office of the Australian Information Commissioner (OAIC) has the power to seek significant court enforced fines for serious or repeated interferences with a person's privacy. The Privacy Commissioner also has a range of other powers, including the power to make a

determination that the Department contravened the Privacy Act. These determinations are publically available on the OAIC's website and can therefore cause reputational harm. The Privacy Commissioner also has the power to conduct privacy assessments and publish the findings of these assessments on the OAIC's website.

Further, personal information that is obtained under the AusCheck scheme or that relates to the administration of the AusCheck scheme is defined to be *AusCheck scheme personal information* under subsection 4(1) of the AusCheck Act.

The use and disclosure of *AusCheck scheme personal information* is subject to even more stringent safeguards under sections 13, 14 and 15 of the AusCheck Act. Sections 13 and 14 of the AusCheck Act are relevant to how information is collected, retained and shared, with section 15 of the AusCheck Act covering the protection of information. These sections of the AusCheck Act have been designed and developed to ensure that the acts and practices of the Secretary, AusCheck and delegates in relation to the disclosure of personal information, are consistent with the Australian Privacy Principles (APP).

Item 10 – Paragraph 5(1)(d)

Item 10 amends paragraph 5(1)(d) of the AusCheck Regulations to add a reference to new Division 3AAB. This amendment is consequential to the amendment made by Item 20.

This amendment inserts a reference to new Division 3AAB inserted by item 20 to provide that an application for a background check for an individual permitted under a CIRMP, residential addresses for the last 10 years before the application is made must be provided.

This information must be provided by an individual or a responsible entity, whichever makes the application to AusCheck, when making an application for a critical infrastructure background check to be conducted under section 21Q (introduced by Item 24 below).

Item 11 – After Paragraph 5(1)(ia)

Item 11 inserts a new paragraph 5(1)(iab) into the AusCheck Regulations, prescribing additional required information to be provided for an application for a *critical infrastructure background check* under section 21Q. This information does not need to be provided for applications relating to aviation and maritime security cards, access to security sensitive biological agents, or major national events.

New paragraph 5(1)(iab) applies whether the application for the critical infrastructure background check is made by an individual or by a responsible entity.

Subparagraph 5(1)(iab) makes clear that if the application for a background check is made in relation to an individual who is, or is to be, employed, and the application relates to a background check of the individual permitted under a CIRMP, the individual or responsible entity making the application must provide the following:

- the name and business address of the responsible entity in relation to whom the CIRMP applies (subparagraph 5(1)(iab)(i)), and

- details of the capacity in which the individual is, or is to be, employed (subparagraph 5(1)(iab)(ii)), and

- if the individual is, or is to be, employed by an entity other than the responsible entity in relation to whom the CIRMP applies—the name and business address of the entity (subparagraph 5(1)(iab)(iii)),and

- the reason the individual is an individual for whom a background check is permitted under the CIRMP (subparagraph 5(1)(iab)(iv)).

In operational terms, this amendment makes clear that if the person is or is to be employed by someone other than a responsible entity, the required information is the name and address of their employer, and the reason why the individual requires unescorted access to the critical infrastructure asset. The requirements in subparagraphs 5(1)(iab)(i) and (ii) are consistent with similar requirements in paragraphs 5(1)(i) or (ia), and the requirement in subparagraph 5(1)(iab)(iii) is consistent with a similar requirement that a person show an 'operational need' in relation to the ASIC and MSIC schemes (see paragraphs 5(1)(h) or (j)).

The purpose and effect of this amendment is to align, to the extent possible, the information required for a background check of an individual that is permitted under a CIRMP, with the information required for background checks conducted for the ASIC/MSIC and major national event schemes.

Item 12 – After paragraph 5(1)(ka)

Item 12 inserts new paragraph 5(1)(kb) into the AusCheck Regulations, prescribing required information to be provided for an application that relates to a background check of the individual permitted under a CIRMP under new section 21Q, where the individual is a student.

Under new paragraph 5(1)(kb), where an application for a critical infrastructure background check is in relation to a student, the application must include:

- the business name and address of the responsible entity in relation to whom the CIRMP applies(sub-paragraph 5(1)(kb)(i)),

- the name and business address of the institution at which the individual is studying (sub-paragraph 5(1)(kb)(ii)),

- details of the work that individual is undertaking, or will undertake, with the responsible entity (sub-paragraph 5(1)(kb)(iii)), and

- the reason the individual is an individual for whom a background check is permitted under the CIRMP (sub-paragraph 5(1)(kb)(iv)).

The information required by new paragraph 5(1)(kb) provides context for AusCheck to conduct and coordinate the critical infrastructure background check, and is consistent with the requirement imposed in existing paragraph 5(1)(ka) in relation to a student making an application for a background check for major national event purposes.

Item 13– After paragraph 5(1)(m)

Item 12 inserts new paragraph 5(1)(ma) which requires an application for a background check of an individual permitted under a CIRMP to include a record of the express consent of the individual for:

- the background check to be conducted, and

- an identity verification check if the CIRMP mandates that identity verification is included in the background check.

The information required by new paragraph 5(1)(ma) ensures the integrity of the scheme by requiring a record of the individual clearly and expressly giving informed consent to a critical infrastructure background check being undertaken.

Item 14 – At the end of subsection 5(1)

Item 14 inserts new paragraph 5(1)(o) which requires an application for a background check of an individual permitted under a CIRMP for an individual under 16 years of age at the time the application is made to include the express consent from a parent or guardian of the individual:

- for the background check to be conducted (sub-paragraph 5(1)(o)(i)), and

- an identity verification check if the CIRMP mandates that identity verification is included in the background check (sub-paragraph 5(1)(o)(ii)).

The information is required as it is an appropriate privacy safeguard for a parent or guardian of a child to provide express consent for background checks, and identity verification checks, to be conducted.

An individual under 16 years of age may be a person undertaking an apprenticeship in or at a critical infrastructure asset, or in relation to the construction, repair, maintenance or sustainment of a critical component of a critical infrastructure asset.

Item 15 – At the end of subsection 5A(1)

Item 15 inserts new paragraph 5A(1)(d) to provide that section 5A does not apply if the requirement relates to a background check of the individual permitted under a CIRMP.

Section 5A provides exemptions from the requirements to provide details of identification documents.

The purpose and effect of this amendment is to create consistency with the major national event scheme in excluding the new *critical infrastructure background check scheme* from the application of section 5A. Identity verification in relation to *critical infrastructure background check* are separately dealt with under Division 3AAB of Part 2 of the AusCheck Regulations, as inserted by the Amendment Regulations under Item 20 of Schedule 1, see further explanation at that Item.

Item 16 – At the end of subsection 5B(2)

Item 16 amends subsection 5B(2) to provide that section 5B does not apply in relation to a background check of an individual permitted under a CIRMP.

Section 5B provides that AusCheck is not required to continue undertaking a background check where AusCheck is unable to verify the identity of the individual in certain circumstances.

This amendment is required because new section 21Y of the AusCheck Regulations separately provides that AusCheck is not required to continue background checking of an individual for the purposes of a *critical infrastructure background check* if that individual's identity is required to be electronically verified and cannot be verified under section 21Y (see further at Item 24).

Items 17 and 18 –subsection 5B(2) (note), (at the end of the note)

Items 17 and 18 make consequential amendments to the guiding note following subsection 5B(2). The purpose and effect is to remind the reader that they should refer to section 21L and new section 21Y (inserted by Item 24, below) for when AusCheck is not required to continue undertaking a background check in relation to CIRMPs.

Item 19 – At the end of section 6

Item 19 inserts new paragraph 6(e) which operates to provide that for an individual for whom a background check is undertaken under new sections 11AD, 11AE or 21DC a person has an *unfavourable criminal history* when the person has a *CIRMP criminal record* (as defined in section 4, see Item 4).

The effect of paragraph 6(e) is to put beyond doubt that in circumstances where a background check of an individual is permitted under a CIRMP, an individual has an *unfavourable*

criminal history if the criminal history of the individual discloses that the person has a *CIRMP criminal record.*

Item 20 – After Division 3AA of Part 2

Item 20 inserts new Division 3AAB into Part 2 of the AusCheck Regulations (containing sections 11AD and 11AE) to provide for the conduct of critical infrastructure background check*s*, by AusCheck, of individuals for whom a *CIRMP* permits a background check.

The operational effect of the critical infrastructure background check is that, in circumstances where a background check is conducted, AusCheck will provide advice to both the individual to whom it relates and the relevant responsible entity about the outcomes of the individual checks undertaken by background checking partners (e.g. Immigration, the Australian Security Intelligence Organisation, and the Australian Federal Police). This advice, along with other considerations, will allow the responsible entity to assess the person's suitability to have unescorted access to the responsible entity's critical infrastructure asset in accordance with the applicable Rules made under the SOCI Act and the responsible entity's risk management program.

Section 11AD – Background check of applicants for, or holders of, critical infrastructure background check *—application by responsible entity etc.*

Subsection 11AD(1)

New subsection 11AD(1) provides a discretion for AusCheck to undertake a *background check* of an individual in circumstances where:

- a CIRMP permits a background check of the individual, and
- an application for a background check of the individual is made under section 21Q.

Applications made by a responsible entity, or an individual as endorsed by a responsible entity, under new section 21Q will be the primary mechanism by which AusCheck will conduct and coordinate *background checks* where a CIRMP permits a background check of the individual. Subsection 11AD(1) provides AusCheck with legislative authority to undertake a *background check* in those circumstances.

Subsection 11AD(2)

New subsection 11AD(2) provides an application for a *background check* (where a CIRMP permits a background check of the individual) must:

- be made electronically, and
- include all of the 'required information' (as defined by section 5 of the AusCheck Regulation as amended by Items 10 -14, as outlined above), and

- include a statement by the responsible entity:
    - as to whether the CIRMP permits or requires an assessment of information relating to one or more of the matters mentioned in paragraphs 5(a), (b), (c) or (d) of the Act, and
    - if the CIRMP permits or requires an assessment of information relating to the matters in paragraph 5(b) of the Act, how the responsible entity deals with an *adverse security assessment* or a *qualified security assessment* under the CIRMP, and
- include the details required under section 21V or a copy of an exemption (or a copy of an application for an exemption) under section 21X from the requirement to provide those details, and the record (if any) required under section 21V if, under the CIRMP, the background check must include an electronic identity verification check, and
- be made in the form (if any) approved for the purposes of subsection 11AD(3), and
- meet any other requirements specified by the Secretary for the purposes of subsection 11AD(4).

The requirement that the application includes a statement by the responsible entity are novel for this background checking scheme. This requirement will indicate to AusCheck that the responsible entity's CIRMP permits background checks to be undertaken and, if so, which of the checks mentioned in paragraphs 5(a), (b), (c) or (d) of the AusCheck Act the CIRMP permits as well as, where relevant, what the CIRMP specifies in relation to how the responsible entity deals with *adverse security assessment* or a *qualified security assessment*.

The purpose and effect of this amendment is to ensure that the requirements specified in subsection 11AD(2) generally align with similar existing requirements imposed by subsection 11AA(2) for major national event purposes, subsection 8(3) for ASIC or MSIC purposes and subsection 11(3) for national health security purposes.

Subsections 11AD(3) and (4)

New subsection 11AD(3) authorises the Secretary to approve the form in which an application under section 21Q must be made, for the purposes of paragraph 11AD(2)(e).

This subsection operates to permit approval to be given for the format of an application, ensuring uniformity in how an application is made and that the requirements specified in subsection 11AD(1) are addressed by the form.

New subsection 11AD(4) provides the Secretary with authority to specify, by notifiable instrument, additional requirements for an application under section 21Q, for the purposes of paragraph 11AD(2)(e).

This subsection operates to give the Secretary a discretion to impose additional requirements for an application made under section 11AD, and is consistent with a similar discretion in subsection 11AA(4). This permits the Secretary to impose additional requirements in relation to particular critical infrastructure assets or sectors to meet their security needs.

Section 11AE – Background checks for critical infrastructure risk management program purposes—deemed application

New subsection 11AE(1) provides AusCheck with a discretionary authority to conduct a new background check of an individual. This subsection applies if the individual has previously been the subject of a critical infrastructure background check conducted under section 11AD, in circumstances where the relevant *CIRMP* permits a background check of the individual and the Secretary considers on reasonable grounds that the individual has a *CIRMP criminal record*.

This subsection makes provision for a further background check to be undertaken in circumstances where:

- the individual has previously been the subject of a critical infrastructure background check conducted under section 11AD (the *original background check*), and
- the Secretary considers, on reasonable grounds, that the individual:
    - has a *CIRMP criminal record*, or
    - if the *original background check* was undertaken for the purpose of granting the individual access to a critical infrastructure asset declared by the Minister via notifiable instrument—constitutes a threat to the security of the declared critical infrastructure asset.

It is necessary for this separate authority to conduct a background check to be prescribed, to empower AusCheck with the discretion to conduct further background checks in circumstances where the Secretary (or delegate) becomes aware of information concerning the relevant individual.

The 'reasonable grounds' referred to in subsection 11AE(1) effectively requires that there is a reasonable basis for the Secretary considering that the person has or had a *CIRMP criminal record* or that the person may constitute a risk to the security of a critical infrastructure asset, and that another person with the same information as the Secretary has would form the same view. This is a prerequisite before the discretion to conduct a background check can be exercised by AusCheck. As an example, the Secretary may receive advice about an individual from a law enforcement or national security agency (see paragraph 11AE(2)(b) below). Depending on the nature and content of the information, receiving such advice might provide a basis for the Secretary's formulation of considering, or holding a particular view in relation to the individual, on 'reasonable grounds' for the purposes of subsection 11AE(1).

Of note, the deemed application relating to security concerns under subparagraph 11AE(1)(b)(ii) is limited in scope—in that it only applies to background checks undertaken for the purpose of granting the individual access to a critical infrastructure asset declared by the Minister. It is intended that this declaration will only be made in limited circumstances where there are particular national security concerns.

For example, more stringent security and integrity requirements are intended to be imposed at current naval shipbuilding assets, and for future naval shipbuilding assets that may become subject to requirements, as set out in the draft *Security of Critical Infrastructure (Naval shipbuilding precinct) Rules (LIN 23/007) 2023*.

Making express provision for the Minister to make a declaration with respect to a critical infrastructure asset by notifiable instrument, rather than stipulating these matters on the face of the legislation has multiple purposes. Primarily, it is to identify which assets carry higher security considerations and would require subsequent background checking if there are reasonable grounds to consider that an individual with access to the asset constitutes a threat to the security of the asset. For example, some critical infrastructure assets will have stringent security controls and will set out appropriate processes and procedures for managing security, and those assets could be declared by the Minister.

The second aspect is that making a declaration about an asset by way of a notifiable instrument permits the Minister to respond quickly to changes in the threat environment for the asset to address or pre-empt any emerging threats.

The third aspect is to recognise that such a declaration is likely to be of long-term public interest for which public accessibility and centralised management is desirable.

And finally, despite notifiable instruments not being subject to the same consultation requirements as legislative instruments, consultation with the relevant responsible entity that has higher security considerations can be conducted.

For example, consultation has been undertaken with the proposed responsible entities for naval shipbuilding assets and with the Department of Defence (the proposed Regulator for that asset under the SOCI Act) in relation to the deemed application that will be available via subparagraph 11AE(1)(b)(ii). It has been commonly agreed that the deemed application is appropriate to ensure that individuals who have access to the asset can be subject to subsequent background checking if relevant security concerns are subsequently identified.

Subsection 11AE(2) prescribes the matters that must be taken into account by the Secretary when considering the matter mentioned in subsection (1). Those matters are:

- any information given to the Secretary by the individual or the relevant responsible entity in relation to whom the CIRMP applies (paragraph (a)),

- any information given to the Secretary by a law enforcement, or national security, agency (however described) about the individual (paragraph (b)), and

- anything else relevant that the Secretary knows about (paragraph (c)).

Subsection 11AE(3) is a deeming provision that operates to provide that, if AusCheck undertakes a background check of an individual under subsection 11AE(1):

- the entity who made the original application (whether that is the responsible entity or the individual) is taken to have applied for the new critical infrastructure background check of the individual, and

- the application for that critical infrastructure background check is taken to be the same as the application for the original background check (paragraph (b)).

This 'deemed application' provision is required to be prescribed so that the powers of the Secretary in relation to the application, for example to request additional information, are enlivened (see section 11A of the AusCheck Regulations). The deemed application provision is also required to enliven AusCheck's capacity to provide advice to an individual or a responsible entity about the outcome of the background check (section 21Q, see Item 24).

A fee described in section 30 of the AusCheck Regulations is not payable in relation to a deemed application under section 11AE.

Item 21 – Paragraph 11A(2)(b)

Subsection 11A(2) of the AusCheck Regulations provides the Secretary with discretionary authority to request that an individual for whom an application for a background check is made, or the body or entity that applied for the background check, to do a specified thing (including the giving of information) upon reasonable suspicion of prescribed circumstances (the circumstances are prescribed in paragraphs 11A(2)(d)-(g)).

Previously, this discretion could be exercised in relation to an ASIC or MSIC issuing body, NHS entity or major national event accreditation organising body that applied for the background check.

In practice, the amendment made by this Item would extend this discretion to permit the Secretary (or a delegate) to request that a thing is done, such as providing further information, by the individual or responsible entity so that a critical infrastructure background check can be conducted.

'Reasonably suspecting' something is a common threshold for the state of mind required before a decision maker takes a particular action. This threshold imposes a requirement that there be reasonable grounds for 'suspecting' that one of the circumstances in paragraphs 11A(2)(d)-(g) exists, and means that the Secretary must suspect that the relevant circumstance exists and that the suspicion is objectively reasonable. Therefore the grounds upon which the suspicion is based must be capable of inducing a similar belief in a reasonable person in the position of the Secretary.

In effect, the amendment made by Item 21 gives the Secretary the authority to request that an individual or responsible entity does a thing specified in the request if the Secretary reasonably suspects that thing is necessary for the purposes of any of the matters listed in paragraphs 11A(2)(d)-(g).

Item 22 – Paragraph 11A(2)(f)

As outlined at Item 21 above, subsection 11A(2), provides the Secretary with authority to request an individual who is the subject of a background check or a responsible entity to do a specified thing upon reasonable suspicion of the circumstances prescribed in paragraphs 11A(2)(d)-(g).

Paragraph 11A(2)(f) of the AusCheck Regulations allows the Secretary to require an individual or relevant authority to do a specified thing where the Secretary reasonably suspects that doing the thing is necessary to meet a requirement prescribed under subsection 11A(3) for a background check made under specified sections of the AusCheck Regulations relating to aviation and maritime transport, national health security, and major national events.

Item 22 amends paragraph 11A(2)(f) so that the paragraph also applies to applications made under new subsection 21DC(5), being a critical infrastructure background check conducted in circumstances where the Secretary reasonably suspects that the original background was conducted on incomplete or inaccurate information (see Item 24).

As a result of the amendments made by this Item and Item 21, the Secretary has capacity to request that an individual or a responsible entity for a critical infrastructure asset do a specified thing to meet any of the requirements specified for the purposes of paragraph 11A(2)(f) of the AusCheck Regulations, where the Secretary reasonably suspects that doing the specified thing is necessary for that purpose.

Item 23 – At the end of Division 5 of Part 2

Division 5 of Part 2 of the AusCheck Regulations prescribes when and to whom the Secretary must provide advice about the outcomes from background checks for aviation and maritime security purposes (Subdivision A), for national health security purposes (Subdivision B), and for major national event purposes (Subdivision C).

Item 23 inserts new Subdivision D into Division 5 of Part 2 of the AusCheck Regulations, incorporating new sections 21DA, 21DB, 21DC and 21DD, prescribing when and to whom the Secretary must provide advice about the outcomes of a critical infrastructure background check.

Subdivision D—Advice about background checks for critical infrastructure risk management programs

New Section 21DA – Advice about background check of an individual

New section 21DA prescribes requirements for the Secretary to provide advice to a responsible entity for a critical infrastructure asset about the outcome of a critical infrastructure background check for an individual, conditional upon what types of assessments for the background check are required to be conducted by the relevant Rules and the requirements set out in the responsible entity's *CIRMP*. For example, the applicable Rules and *CIRMP* may require that an assessment of some or all of the following are included in the background check (as defined by paragraph 5(a), (b), (c) and (d) of the AusCheck Act):

- the individual's criminal history,
- matters relevant to a security assessment of the individual (as defined in subsection 35(1) of the *Australian Security Intelligence Organisation Act 1979*),
- the individual's citizenship status, residency status or entitlement to work in Australia, including but not limited to, whether the person is an Australian citizen, a permanent resident or an unlawful non-citizen, and
- the identity of the individual.

Subsection 21DA(1)

Subsection 21DA(1) provides 21DA applies if AusCheck undertakes a background check of an individual under new sections 11AD, 11AE or 21DC.

Advice relating to criminal history etc.

Subsection 21DA(2)

New subsection 21DA(2) operates to prescribe what the Secretary must advise the responsible entity of in relation to an individual to whom the CIRMP applies.

Under paragraph 21DA(2)(a), if a background check includes an assessment of the individual's criminal history, it is mandatory that the Secretary advises the responsible entity whether or not the individual has an *unfavourable criminal history*. Further detail about the outcome of a criminal history check may also be required to be provided by the Secretary under subsection 21DA(3) (see below).

This advice is important for a responsible entity to know. For example, if the individual has been convicted of (or convicted of and sentenced for) an offence listed as a *critical infrastructure risk management program-security-relevant offence* as newly set out in Schedule 2 to the AusCheck Regulations (see Item 27), this may be something considered by the responsible entity when making an assessment in relation to the individual's suitability to

have unescorted access to the relevant critical infrastructure asset according to the risk profile set out in its risk management program.

Under paragraph 21DA(2)(b), if the background check included a security assessment of the individual, it is mandatory that the Secretary advises the responsible entity whether or not the individual has an *adverse security assessment* or a *qualified security assessment* (defined in section 4 of the AusCheck Regulations by reference to the meaning of those terms in Part IV of the *Australian Security Intelligence Organisation Act 1979*).

This advice is important for a responsible entity to know for the same reason as for paragraph 21DA(2)(a). That is, if advice is provided that an individual has an *adverse security assessment* or a *qualified security assessment*, then the responsible entity will need to consider that information in accordance with their processes and systems to manage personnel hazards as set out in the entity's CIRMP.

Under paragraph 21DA(2)(c), if the background check included an assessment of information relating to whether the individual is an unlawful non-citizen or holds a visa entitling the individual to work in Australia, it is mandatory that the Secretary advises the responsible entity whether or not the individual has a right to work in Australia, and if so, the class of visa held.

A person can legally work in Australia if they are an Australian citizen or permanent resident or a New Zealand citizen, or they hold a valid visa with permission to work. This advice is important for a responsible entity to know as an employer who employs a person who is an unlawful non-citizen or who holds a visa that is subject to a work-related condition may be committing an offence under the *Migration Act 1958* and may be subject to a criminal or a civil penalty. For example a contravention of section 245AB, or section 245AC, of the *Migration Act 1958* each carry a criminal penalty of 2 years imprisonment and a civil penalty of 90 penalty units (at the time of writing, each penalty unit is the indexed amount of $222 in accordance with subsection 4AA(3) of the *Crimes Act*).

This advice specified in section 21DA is consistent with advice specified in relation to other background checking schemes.

Subsection 21DA(3)

New subsection 21DA(3) makes it mandatory that if Secretary advises the responsible entity under paragraph 21DA(2)(a) that the individual has an unfavourable criminal history, the Secretary must include in the advice details of the type of offence of which the individual has been convicted, and must inform the individual of that advice and the reasons for that advice.

This advice given under subsection 21DA(3) only includes details of the type of offence and does not include giving the responsible entity details of the offence of which the individual has been convicted as this is subject to the further consent requirements outlined in subsection 21DA(5).

The advice given under subsection 21DA(3) will only refer to the date and type of offence referring back to the offences listed in the tables in Schedule 2 (as introduced by Item 27 below). The advice not give the responsible entity details of the offence of which the individual has been convicted as this is subject to the further consent requirements outlined in subsection 21DA(5).

The advice is given to the individual at the same time as the responsible entity to ensure transparency of AusCheck advice, and allow the individual and the responsible entity to manage any risk identified as a result of the background check in accordance with their CIRMP.

Similarly to subsection 21DA(2), subsection 21DA(3) engages the exception in Australian Privacy Principle (APP) 6.2(b), which allows for secondary use or disclosure of personal information which is required or authorised by law. Advice given under subsection 21DA(3) is disclosing a fact about the existence of sensitive information to the responsible entity, rather disclosing the sensitive information itself.

Subsection 21DA(4)

New subsection 21DA(4) makes it mandatory that the Secretary provides advice to the responsible entity with respect to whether there has been a material change in the individual's criminal history if:

- the Secretary has advised the responsible entity in relation to a previous background check of the individual, and

- the advice in relation to the previous background check was that the individual had an unfavourable criminal history.

This advice is important for a responsible entity to know for the same reason as for paragraph 21DA(2). That is, if advice is provided that there has been a material change in individual's criminal history since the previous background check was conducted then the responsible entity may consider this matter when making an assessment in relation to the individual's suitability to have unescorted access to the relevant critical infrastructure asset according to the risk profile set out in its risk management program.

Similarly to subsection 21DA(3), subsection 21DA(4) engages the exception in Australian Privacy Principle (APP) 6.2(b), which allows for secondary use or disclosure of personal information which is required or authorised by law. Advice given under subsection 21DA(4) is disclosing a fact about the existence of sensitive information to the responsible entity, rather disclosing the sensitive information itself.

The intention of subsection 21DA(4) is to enable a responsible entity to consider any material changes in an individual's criminal history in its risk assessment processes prior to deciding whether to give the individual unescorted access to its critical infrastructure asset.

Subsection 21DA(5)

New subsection 21DA(5) makes it mandatory that the Secretary provides to the responsible entity a document setting out the details of *CIRMP offence* an individual has been convicted of, as well as any sentence imposed for the offence, if:

- the Secretary has advised the responsible entity that an individual has been convicted of a *CIRMP offence* pursuant to paragraph 21DA(3)(a) (paragraph (a)), and

- the responsible entity makes a written request to the Secretary to provide the responsible entity with the details with the offence of which the individual has been convicted (paragraph (b)), and

- the individual provides express consent for the Secretary to provide details of the *CIRMP* offence to the responsible entity (paragraph (c)). This is an important measure by which the individual will be aware of, and provide consent for, the disclosure of their personal and sensitive information (within the meaning of the *Privacy Act 1988*).

The intention of subsection 21DA(5) is to enable a responsible entity to fully consider an individual's relevant criminal history in its risk assessment processes prior to deciding whether to give the individual unescorted access to its critical infrastructure asset. Subsection 21DA(5) also provides a safeguard to the individual by protecting that information unless the individual expressly consents to the disclosure.

The purpose of this amendment, and other amendments made by this instrument is to assist responsible entities to reduce, and where possible eliminate, personnel security risks to their own *critical infrastructure asset* which, due to the interconnectedness of some industries, may also provide protection to the operations of one or more other *critical infrastructure assets.*

Giving advice to a responsible entity that a person has an *unfavourable criminal history*, an *adverse security assessment* or *qualified security assessment* is therefore reasonable, necessary and proportionate to achieving this legitimate aim, paying due regard to the nature of the relevant information and the overall objectives of the critical infrastructure background checking scheme.

Personal information collected by the discrete area within the Department that performs the AusCheck function (AusCheck), including the outcome of a critical infrastructure background check, is protected under the AusCheck Act and AusCheck Regulations. Sections 13 and 14 of the AusCheck Act are relevant to how information is collected, retained and shared, with section 15 of the AusCheck Act covering the protection of information. As noted above in relation to *required information*, these sections of the AusCheck Act have been designed and developed to ensure that the acts and practices of the Secretary, AusCheck and delegates in relation to the disclosure of personal information, are consistent with the APPs, which are the cornerstone of the Privacy Act.

Privacy Act and AusCheck Act

The Privacy Act applies in relation to this amendment. However, the effect of this provision is that disclosure of personal information by AusCheck to a responsible entity in those particular circumstances will be required by law.

APP 6 of Part 3 of Schedule 1 to the Privacy Act generally governs the use and disclosure of personal information by an APP entity, such as the Department (and by extension, AusCheck by virtue of being a discrete area within the Department). In particular, APP 6.1 provides that an APP entity must not use or disclose personal information about an individual that was collected for a particular purpose for another purpose, unless the individual has consented or an exception applies. Such exceptions to the prohibition on use or disclosure include where a disclosure is required or authorised by or under Australian law (APP 6.2(b)). In effect, this means the amendments in new section 21DA have the consequence that the required disclosures will be consistent with the requirements of APP 6.

However, the personal information the Secretary must disclose to responsible entities will also be *AusCheck scheme personal information* (as defined in subsection 4(1) of the AusCheck Act). The use and disclosure of *AusCheck scheme personal information* is subject to even more stringent safeguards under sections 13, 14 and 15 of the AusCheck Act.

In particular, subsection 15(1A) of the AusCheck Act provides that it is a criminal offence punishable by two years' imprisonment if a person obtains information that is AusCheck scheme personal information and the person discloses that information to someone else, unless an exception under subsection 15(2) applies. Importantly, the offence in subsection 15(1A) continues to apply to the on-disclosure of AusCheck scheme personal information. The effect of this is that, where AusCheck scheme personal information is disclosed to a responsible entity in accordance with the new section 21DA, it will be an offence for the responsible entity to disclose the AusCheck scheme personal information unless an exception in subsection 15(2) applies. The exceptions in subsection 15(2) include disclosures:

- made with consent of the relevant individual,
- to the individual to whom the AusCheck scheme personal information relates,
- taken to be authorised by section 13, authorised under section 14 or required or authorised by another law, or
- to Australian Federal Police for the purposes of the AusCheck scheme.

Disclosures (and use) authorised by section 14 are generally for the purposes of, or in connection with, the AusCheck scheme, or for specific purposes, such as for the purposes of responding to an incident that poses a threat to national security or the performance of functions relating to law enforcement or national security by the Commonwealth, a State or Territory (or an authority of Commonwealth, a State or Territory).

Therefore whilst section 21DA will have the effect that the disclosure of information by the Secretary to the responsible entity without the relevant individual's consent, given the more limited purposes for which AusCheck scheme personal information can be used and disclosed under the AusCheck Act (and the offence provision in subsection 15(1A) of the AusCheck Act), the information that may be disclosed is subject to more rigorous safeguards.

Other safeguards

Section 13 of the AusCheck Regulations specifies what information must be shared and with whom, when AusCheck provides advice about a background check for an individual for critical infrastructure purposes. Subsections 13(2), 13(3) and 13(4) specifically set out what advice relating to criminal history must be given, for example, only the advice that the individual has an *unfavourable criminal history*, or that and *adverse security assessment* has been given in relation to the person must be given to a responsible entity, thereby providing the relevant safeguards.

Section 21DB – Advice about a background check that is cancelled

New section 21DB prescribes the circumstances in which it is mandatory that the Secretary gives advice to an individual or a responsible entity (as the case requires) that the background check for the individual is cancelled. This section is intended to be conjunctive, meaning that advice may be provided to an individual, to a responsible entity, or to both the individual and the responsible entity.

Advice under section 21DB must be provided where:

- a background check of an individual is cancelled under subsection 11A(7) (paragraph (a)), and
- had AusCheck completed the check, the Secretary would have been required or authorised (whether or not doing so would have been dependent upon the results of the check) to give the individual or the responsible entity to whom the *CIRMP* that permits the background check applies advice (subparagraph (b)(i)) or a document (subparagraph (b)(ii)).

An example of circumstances where such advice may be given is when the Secretary makes a request under subsection 11A(2) of the AusCheck Regulations for the individual or responsible entity to do a specified thing, and the thing is not done by the specified date for complying with the specified thing. This could then result in cancellation of the background check under subsection 11A(7).

New section 21DB is analogous to sections 15A and 21B of the AusCheck Regulations, which currently make similar provision requiring the Secretary to provide advice in respect of cancelled applications for background checks for aviation and maritime security or major national event purposes, respectively.

Section 21DC – AusCheck may undertake new background checks

New section 21DC of the AusCheck Regulations provides AusCheck with statutory authority to conduct a new background check of an individual to which subsection 21DC(1) or (2) applies.

Section 21DC prescribes the circumstances in which AusCheck may undertake a new background check after giving advice about the outcome of 'the original' background check conducted under Subdivision D of Division 5 of Part 2 (in particular, under subsection 21DA(2) or section 21DB).

Subsection 21DC(1)

New subsection 21DC(1) provides that the section applies if the Secretary gives advice about a background check (referred to as the original check) of an individual under new Subdivision D (i.e. under sections 21DA, 21DB or 21DD), and the Secretary later reasonably suspects that one or more of the four circumstances prescribed in subparagraphs 21DC(b)(i)-(iv) apply, namely:

- any of the requirements for the application (made under section 21Q) for the original background check (specified in subsection 11AD(2), outlined at Item 20 above) were not satisfied

- the Secretary did not have all the required information (as defined by section 5 of the AusCheck Regulations as amended by Items 10 to 14) for the individual when AusCheck undertook the original check

- any of the requirements specified under subsection 11A(3) for the purposes of paragraph 11A(2)(f) in relation to the application for the original check were not satisfied, or

- the advice provided by the Secretary under new Subdivision D is inaccurate or incomplete.

The state of mind threshold requiring that the Secretary 'reasonably suspects' the existence of any of the four circumstances prescribed in subparagraphs 21DC(b)(i)-(iv) imposes a requirement that there be reasonable grounds for 'suspecting' that one of the circumstances exists. This threshold means that the Secretary must suspect that the relevant circumstance exists and that the suspicion held by the Secretary is objectively reasonable. The grounds upon which the suspicion is based must be capable of inducing a similar belief in a reasonable person in the position of the Secretary.

Subsection 21DC(2)

Subsection 21DC(2) makes clear that this section also applies if the Secretary cancels a background check of an individual under subsection 11A(7) and gives advice of the

cancellation under section 21DB and the thing that the Secretary requested be done under subsection 11A(2) in relation to the cancelled background check is later done.

This will permit a background check to be undertaken relying on the additional information or other 'thing', despite the information or other thing not being provided by the date specified in the request made under subsection 11A(2).

Subsection 21DC(3)

Subsection 21DC(3) makes clear that this section also applies if an individual informs the Secretary, as they are required to do under new section 21ZB (inserted by Item 24 below), that the individual has been convicted of a CIRMP level 1 offence or has been convicted of a *CIRMP level 2 offence* and sentenced to any term of imprisonment for the offence.

This will permit a background check to be undertaken where an individual makes a relevant disclosure under new section 21ZB.

Subsection 21DC(4)

Subsection 21DC(4) is an enabling provision that explicitly provides AusCheck with the discretion to undertake a new background check of the individual in the circumstances mentioned in subsections 21DC(1), (2) and (3).

Subsection 21DC(5)

Subsection 21DC(5) is a deeming provision that provides that if AusCheck undertakes a new background check (enabled by subsection 21DC(3)) for the purposes of the AusCheck scheme:

- the applicant for the original background check (i.e. the individual or the responsible entity) is taken to have applied for the new background check (paragraph (a)), and
- the application for the new background check is taken to be the same as the application for the original check (if any) (as affected by subsection 11A(6)) (paragraph (b)). That is, the deemed application would include any information given to the Secretary in response to a request to do a specified thing under subsection 11A(2).

The guiding note after subsection 21DC(5) reminds the reader that paragraph 21DC(5)(b) may be relevant to whether the Secretary may make a request under subsection 11A(2) in relation to the application.

Subsection 21DC(5) is included so that AusCheck is expressly empowered to undertake a new background check on an individual that includes any information received after the Secretary has exercised their powers under section 11A of the AusCheck Regulations. This

new background check would generate new 'advice' that may be given to a responsible entity or the individual to whom it relates, see section 21DD below.

Section 21DC is analogous to sections 16A, 20B and 21C of the AusCheck Regulations, relating to aviation and maritime security background checks, national health security background checks, and major national events background checks, respectively.

The purpose of section 21DC is to ensure that background checks are properly conducted, considering all relevant information, so that accurate advice can be given to responsible entities and individuals on the basis of those background checks, which will improve security outcomes. This purpose is achieved by giving AusCheck the power to undertake a new background check where it becomes apparent that any of the requirements for the application for the original background check were not satisfied, or the required information for the original background check was inaccurate or incomplete.

Section 21DD – Secretary must give further advice if initial advice is inaccurate or incomplete

New section 21DD prescribes that, if the Secretary becomes aware that advice about a background check of an individual that has been given under Subdivision D is inaccurate or incomplete, the Secretary must give further advice in accordance with Subdivision D that is accurate and complete.

Such initial advice may have been given when the criminal history of an individual did not disclose all their convictions for *CIRMP-security-related offences*, meaning that subsequent advice about the criminal history (in particular whether an individual has been convicted of a *CIRMP level 1 offence* set out in Item 1 of Schedule 2, introduced by Item 27 below) needs to be given by the Secretary to the responsible entity.

This section is analogous to sections 17, 21 and 21D of the AusCheck Regulations, relating to aviation and maritime security background checks, national health security background checks, and major national event background checks respectively.

Item 24 – After Division 5A of Part 2

Item 24 inserts new Division 5B into Part 2 of the AusCheck Regulations, which contains Subdivisions A and B for matters relating to a CIRMP that permits a background check to be conducted in relation to an individual.

Division 5B—Matters relating to critical infrastructure risk management programs

Subdivision A—Applying for background checks and requirements for identity verification checks

Subdivision A provides for the provision of an application (section 21Q) and other identity verification information (sections 21V and 21W) by a responsible entity or an individual to AusCheck so that AusCheck can conduct background checks. This subdivision also deals with the situation where required information cannot be provided (sections 21X and 21Y).

Section 21Q – Arranging for a background check

New section 21Q provides that an individual or a responsible entity to whom the *CIRMP* applies may apply to AusCheck for a critical infrastructure background check if a CIRMP permits a background check of the individual. An application under section 21Q will need to meet the requirements of subsection 11AD(2) of the AusCheck Regulations (see above).

This amendment is an enabling provision that expressly permits an application to be made for a critical infrastructure background check, which is consistent with similar provisions for making background checks under other background checking schemes (for example section 21G enables an organising body for a major national event to make an application for a background check of an individual in connection with the accreditation of the individual in relation to the major national event.)

Section 21V – Electronic identity verification checks

Subsection 21V(1)

New subsection 21V(1) is an enabling provision that operates to provide that the section applies if a *CIRMP* both permits a background check of an individual and provides that the background check must include an *electronic identity verification check*.

Subsection 21V(2)

New subsection 21V(2) operates to limit the application of the requirement that an electronic identity verification check is conducted.

This subsection operates to provide that AusCheck must not conduct the *electronic identity verification check* unless, subject to an exemption given under section 21X (introduced below), the following are provided to AusCheck:

- details of a Category A identification document or a Category B identification document which AusCheck can use to electronically verify the individual's identity (paragraph (a)), and

- if the individual is at least 16 years old at the time of the check—a record of the individual having given express consent to their identity document being verified (paragraph (b)).

This subsection would prevent the requirement being imposed if the details of the Category A or B identification documents cannot be used to verify the individuals' identity electronically and, for individuals over 16, if they have not given their express consent for electronic identity verification.

If an individual is under the age of 16, a record of their parent or guardian having given express consent to the identity document being verified has already been provided as part of the 'required information' to apply for a background check and in particular an identity verification check under section 21Q (see new paragraph 5(1)(o), further detail at Item 10 above). No further consent would need to be specifically obtained for an individual under the age of 16 for the purposes of section 21V.

Given that Category A and Category B identification documents may contain personal information that is 'sensitive information' for the purposes of the Privacy Act (see subsection 6(1)) of that Act), obtaining consent of an individual to use that information to verify their identity is a requirement of the service that AusCheck uses to electronically verify identity documents and an important safeguard against the improper collection and use of that information. This information becomes *AusCheck scheme personal information* under subsection 4(1) of the AusCheck Act that is subject to the comprehensive safeguards granted to *AusCheck scheme personal information* by sections 13, 14 and 15 of the AusCheck Act.

Section 21W– Identity verification checks—in person identity verification

New section 21W prescribes the requirements for conducting an in person identity verification check as part of a critical infrastructure background check.

Subsection 21W(1)

Subsection 21W(1) provides that if a *CIRMP* permits a background check of an individual and provides that the background check must include an in person identity verification check, the check must be conducted in accordance with section 21W.

Subsection 21W(2) individuals who are 18 years of age or older

Subsection 21W(2) operates to provide that an individual who is at least 18 years of age at the time the in person identity verification check is conducted must attend the identity verification check in person and give to the verifying person (being AusCheck, the responsible entity, or a person authorised by AusCheck or the responsible entity to conduct an in person identity verification, as defined in section 4) the information prescribed in paragraphs (2)(a) and (2)(b).

Under paragraph 21W(2)(a), the following documents must be provided to the verifying person at an in person identity verification check:

- a Category A identification document;
- a Category B identification document that is different to the Category A document;
- a Category C identification document that is different to both the Category A and B documents;
- if evidence of the individual's current residential address is not set out in a document already given, a Category D identification document (subparagraph (iv)) that provides that address.

Paragraph 21W(2)(b), further provides that if an individual had completed an electronic identity verification check under new section 21W before attending the in person identity verification check, the individual must provide the identity documents that were used to electronically verify the individual's identity.

The requirements imposed under paragraph 21W(2)(a) adopt a standard of proof of identity consistent with the National Identity Proofing Guidelines. Only original documents can be provided under this subsection, there being no provision allowing for copies or certified copies of the original documents to be provided.

Any documents provided for the purposes of paragraph 21W(2)(b), being a Category A identification document and a Category B identification document (as outlined in new subsection 21V(2)), can also be the documents provided under subparagraphs 21X(2)(a)(i) and (ii). Separate documents would not need to be provided.

Subsection 21W(3) individuals under 18 years of age

Subsection 21W(3) operates to provide that, subject to any exemption given under section 21X, if an individual is under 18 years of age at the time the in person identity verification check is conducted, the individual must attend the identity verification check in person and give to the verifying person:

- a Category A identification document, and
- if the individual's identity has been verified electronically before the in person identity verification check has been conducted—the identity documents that were used to electronically verify the individual's identity.

Subsection 21W(4) Identity to be verified at time the individual attends the check

Subsection 21W(4) operates to provide that the verifying person conducting the in person identity verification check must verify the individual's identity at the time the individual

attends the check, unless the individual is exempted under section 21X from the requirement to attend the identity verification check in person.

This subsection makes clear when the individual's identity must be verified by the verifying person, except in circumstances where the individual has a section 21X exemption from in person attendance, which may be where the person is physically unable to attend for example due to disability or remote locality.

Subsection 21W(5) Identification documents must be provided for each identity verification

Subsection 21W(5) is an 'avoidance of doubt' provision that makes clear that the individual must give the documents referred to in subsection 21W(2) or (3) to the verifying person conducting the in person identity verification check even if the individual has previously given the same documents to the verifying person, or to a verifying person, in relation to another background check permitted under the CIRMP or any other CIRMP.

Section 21X– Exemptions

New section 21X enables an applicant who cannot provide particular identification documents, or who cannot attend an in person identity verification check, to seek an exemption from doing so, in specified circumstances. This provision is analogous to section 21K which makes similar exemptions in relation to major national events accreditation applicants.

Subsection 21X(1) Exemptions

New subsection 21X(1) is an application provision that operates to provide for the circumstances in which the section applies.

Electronic identity verification

Paragraph 21X(1)(a) provides that section 21X applies if, for the purposes of an identity verification check under section 21V or 21W, an individual for whom a CIRMP permits a background check to be conducted is unable to provide details of a Category A identification document or a Category B identification document, being details AusCheck can use to verify electronically the individual's identity for the purposes of a background check (i.e. for the purposes of subsection 21V(2)).

In person identity verification

Paragraph 21X(1)(a) provides that section 21X applies if, for the purposes of an identity verification check under section 21V or 21W, an individual for whom a CIRMP permits a background check to be conducted is unable to provide a Category A identification document at an in person identity verification check, or attend an in person identity verification check (under section 21W).

Subsection 21X(2)

New subsection 21X(2) provides that an individual or responsible entity to whom section 21X applies may apply for an exemption:

- to provide details of a Category A identification document or details of a Category B identification document;
- to provide a Category A identification document,
- to attend the identity verification check in person.

It is anticipated that these exemptions may be required in circumstances where:

- an individual's Category A identification document or a Category B identification document has not been digitised by the document issuer and cannot be electronically verified using the Document Verification System;
- an individual does not hold a Category A identification document and cannot feasibly obtain it in time for a background check to be completed – for example a long term permanent resident, or
- an individual cannot physically attend the location where an in person identity verification check is being held – for example if an individual lives in a remote area or has a disability.

The Category A and Category B identification documents that can be verified using the Document Verification System include an individual's:

- Drivers Licence,
- Passport,
- Medicare Card,
- Centrelink Card,
- Visa,
- ImmiCard,
- Birth Certificate,
- Marriage & Name Change Certificates,
- Citizenship Certificate,
- Registration of Descent Certificate.

If an individual requires an exemption, subsection 21X(2) enables the individual or responsible entity to apply to the Secretary, currently the Secretary of the Department of Home Affairs, for the exemption.

Requirements for application

In making such an application the individual must meet the requirements prescribed in subsection 21X(3). Those requirements are that the application:

- be made electronically, and
- state what exemption is required (outlined in subsection 21X(2)), and
- set out the reasons why the exemption is required, and
- if the application is for an exemption from the requirement to attend an identity verification in person, include:
    - a photograph of the individual, less than a month old, showing the individual's full face and, head and shoulders,
    - certified (in accordance with subsection 21X(4)) copies of the documents required under subsections 21W(2) or (3) that would otherwise be required to be presented in person at the identity check, and
- any other information that may assist the Secretary in making a decision to grant an exemption.

Certification of documents

Subsection 21X(4) provides that, for the purposes of subparagraph 21X(3)(d)(ii), a copy of an identification document must be certified, in writing, by a person prescribed by section 7 of the *Statutory Declarations Regulations 2018,* to be a true copy of the original identification document. Such persons include a Commonwealth public servant with 5 or more years of continuous service, legal practitioner, justice of the peace and a police officer.

Matters to be considered

Subsection 21X(5) specifies matters that the Secretary must consider in making a decision to grant an exemption to an individual under section 21X. Those matters include the reasons set out in the application under paragraph 21X(3)(c), and any other information provided by the individual under paragraph 21K(3)(e).

Requirement for further information

Subsection 21X(6) is an enabling provision that expressly permits the Secretary, if they require further information to consider their decision, to request further information be given by the applicant within 30 days of that request.

When decision must be made

Subsection 21X(7) prescribes the timeframe in which a decision by the Secretary to grant or to refuse to grant an exemption under section 21X must be made and how the decision is to be provided.

Under this subsection, the Secretary must, in writing and within 30 days of receiving the application under subsection 21X(2), unless the Secretary had made a request under subsection 21X(6) for further information:

- grant the exemption in relation to the individual or refuse to grant the exemption in relation to the individual, and
- notify the applicant of the decision, and
- if the decision is a refusal, notify the applicant of the reasons for the refusal.

Subsection 21X(8)

Subsection 21X(8) is a deeming provision that provides the Secretary is taken to have refused to grant the exemption if the Secretary has not made a decision on the application within the period mentioned in subsection 21X(7). This provision will provide certainty to an applicant with respect to when their application for an exemption will be decided.

A decision of the Secretary to refuse to grant an exemption under section 21X (whether by written notice under subsection 21X(7) or a deemed refusal under subsection 21X(8)) is subject to review by the Administrative Appeals Tribunal (see section 26 of the AusCheck Regulations as amended by Item 25, below).

Section 21X is analogous to sections 5A and 21K of the AusCheck Regulations, which currently make similar provisions allowing the Secretary to provide an exemption with respect to providing certain information for identity checks to be conducted in relation applications for background checks for aviation and maritime security, national health security, and major national event purposes.

Section 21Y– AusCheck not required to continue background check if identity not verified

Section 21Y expressly provides authority for AusCheck to not continue a background check of an individual for whom a CIRMP permits a background check to be conducted in circumstances where the individual's identity cannot be verified in accordance with section 21V (or an exemption is not granted under new section 21X).

This would include circumstances where an individual has had an application for an exemption under section 21X refused, or where the individual cannot meet the any requirements of such an exemption, or where an individual has not made an application for an exemption.

Subdivision B— Provision of information relating to background checks for critical infrastructure risk management program purposes

Subdivision B introduces new offence provisions in sections 21ZA and 21ZB.

Section 21ZA applies in respect to the circumstances in which a responsible entity must inform the Secretary of certain decisions the responsible entity takes.

Section 21ZB applies to certain individuals who are required to inform Secretary of certain CIRMP-security-relevant offences.

These offences are novel for the AusCheck Regulations, but share some similarities with provisions in the *Aviation Transport Security Regulations 2005* (ATSR) and *Maritime Transport and Offshore Facilities Security Regulations 2003* (MTOFSR) that require an ASIC or MSIC issuing body to notify the Secretary of certain decisions, such as a refusal to issue a security identification card to an applicant after a background check has been conducted, and those that require an ASIC or MSIC holder to notify the Secretary of convictions or sentences for certain offences if they arise after a background check has been conducted. However, the ASIC and MSIC schemes in the ATSR and MTOFSR differ from the critical infrastructure background checking scheme in the AusCheck Regulations in one significant respect. Those schemes require that an ASIC or MSIC is not issued in circumstances where the applicant or holder of the ASIC or MSIC has an unfavourable criminal history or is the subject of an adverse or qualified security assessment because of the security regulated settings in security controlled airports and ports.

The critical infrastructure background checking scheme complements the requirements of Rules made under the SOCI Act and the responsible entity's CIRMP. The purpose of this scheme is to assist responsible entities to manage, mitigate and control their own specific personnel risk. In effect, the ultimate decision about an individual's suitability to have unescorted access to a responsible entity's critical infrastructure asset is made by the responsible entity after consideration of the background check advice given by the Secretary.

Section 21ZA – Responsible entity must inform Secretary of certain decisions

Decision to grant access to certain assets

New subsection 21ZA(1) prescribes an offence with conjunctive elements that applies in relation to a responsible entity when:

- the Secretary advises the responsible entity about the outcome of a background check of an individual under sections 21DA or 21DD, and

- in the advice, the Secretary advises that the individual has an unfavourable criminal history, or the security assessment of the individual is an *adverse security assessment* or *qualified security assessment*, and

- after receiving advice under sections 21DA or 21DD, the responsible entity makes a decision to grant, or continue to grant, the individual access to a critical infrastructure asset declared by the Minister, by notifiable instrument, for the purposes of paragraph 21ZA(1)(c), and

- the responsible entity does not inform the Secretary of the decision within 7 days of making the decision.

Advice from the responsible entity in the abovementioned circumstances is required to be provided to the Secretary so that AusCheck can maintain an up to date database which is used for law enforcement and national security purposes, and assists the Secretary to determine whether a further check is or may be required under section 11AE.

The offence in new subsection 21ZA(1) carries a penalty of 5 penalty units for failure to comply with the obligation within the 7 day timeframe.

New paragraph 21ZA(1)(c) makes clear that the offence in subsection (1) applies where advice was given to the responsible entity that the individual has an unfavourable criminal history, or an *adverse security assessment* or *qualified security assessment*, and the responsible entity decides to grant, or continue to grant, the individual access to the asset but does not notify the inform the Secretary with the 7 day timeframe.

The offence in subsection 21ZA(1) does not apply if after a background check under section 21DA or 21DD the individual was not granted access, or did not continue to be granted access, to a critical infrastructure asset declared by the Minister for the purposes of paragraph 21ZA(1)(c).

Decision to revoke access to certain assets

New subsection 21ZA(2) prescribes an offence with conjunctive elements that applies in relation to a responsible entity when the responsible entity:

- makes a decision to grant, or continue to grant, an individual access to a critical infrastructure asset of a kind declared by the Minister for the purposes of paragraph 21ZA(1)(c), and

- later makes a decision to revoke the individual's access to the asset, and

- does not inform the Secretary of the decision within 48 hours after making the decision.

The offence in new subsection 21ZA(2) also carries a penalty of 5 penalty units for failure to comply with the obligation within the 48 hour timeframe.

New paragraph 21ZA(2)(c) makes clear that the offence in subsection (2) applies if the individual was granted access, or their previous grant of access continued, in relation to an

asset declared for the purposes of paragraph 21ZA(1)(c), and the responsible entity later decided to revoke that access but did not inform the Secretary with the 48 hour timeframe.

The offence in subsection 21ZA(2) does not apply if the responsible entity does not decide to revoke the individual's previously granted access to the critical infrastructure asset.

The imposition of penalties for breach of offence provisions prescribed in the AusCheck Regulations is expressly authorised by paragraph 18(2)(c) of the AusCheck Act. The maximum penalty that could be imposed on an individual for a contravention of section 21ZA offence would be 5 penalty units, which is within the 50 penalty unit threshold for offences prescribed in regulations, as outlined at paragraph 3.3 of the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (the Guide).

The body corporate multiplier rule set out in subsection 4B(3) of the Crimes Act provides that the maximum penalty that can be imposed on a body corporate (by a court) is five times higher than the penalty that can be imposed on a natural person, meaning that for a corporate entity, the maximum penalty that could be imposed would be increased to 25 penalty units. The only exception to this rule is where, as a matter of law, only a corporation can commit an offence in which case the multiplier does not apply and a correspondingly higher penalty should be specified. In general, a responsible entity would be a corporate entity.

The primary purpose of these 5 penalty unit penalties is to recognise the seriousness of the risk of damage or danger to a critical infrastructure asset or its operations in particular, and the possible flow on effect that damage to, or disruption of, one asset may have on interdependent critical infrastructure assets and the essential services that they provide to Australians more generally. An example of the flow on effect might be where damage is done or disruption occurs at a particular logistics company and the effect that may have on the stocks of grocery or essential medical supplies in each of the states and territories.

The penalty for this offence is lower than penalties for certain comparable offences relating to aviation security functions (being 10 penalty units, see regulation 6.43 of the ATSR in relation to an issuing body telling the Secretary about a decision to cancel an ASIC). Given, however, that responsible entities for a critical infrastructure asset seek AusCheck's background checking services on a voluntary basis and it is in the interests of the security of critical assets and the essential services they provide to encourage participation in the AusCheck scheme, this lower penalty is being imposed.

The intention of imposing a penalty for a failure to inform the Secretary of certain decisions within the specified timeframes in section 21ZA is to ensure that a responsible entity is generally encouraged to comply with those obligations. The offence applies for each instance that the responsible entity fails to notify the Secretary of a decision to approve or refuse to approve a person's access to their asset, or where access is revoked, within the specified time periods.

21ZB Individual must inform Secretary of certain CIRMP-security-relevant offences

Subsection 21ZB(1)

CIRMP level 1 offence—conviction

New subsection 21ZB(1) prescribes an offence with conjunctive elements that applies in relation to an individual when:

- advice has been given to a responsible entity by the Secretary about a background check of the individual under section 21DA or 21DD, and
- after receiving the advice, the responsible entity makes a decision to grant, or continue to grant, the individual access to a critical infrastructure asset declared by the Minister, by notifiable instrument, for the purposes of paragraph 21ZB(1)(b), and
- during the period of 2 years beginning on the day the Secretary gives the advice, the individual is convicted of a *CIRMP level 1 offence* (set out in the table at clause 1 of Schedule 2, see Item 27 below), and
- the individual does not tell the Secretary in writing, within 7 days after individual is convicted, the individual's name, date of birth and residential address, the date the individual was convicted and the court in which the individual was convicted.

The offence in new subsection 21ZB(1) carries a penalty of 5 penalty units for failure to comply with the obligation within the 7 day timeframe.

New paragraph 21ZB(1(b)) makes clear that the offence in subsection (1) does not apply if after a background check under section 21DA or 21DD the individual was not granted access, or did not continued to be granted access, to a critical infrastructure asset declared by the Minister for the purposes of paragraph 21ZB(1)(b).

Subsection 21ZB(2)

CIRMP level 2 offence—conviction and imprisonment

New subsection 21ZB(2) prescribes an offence with conjunctive elements that applies in relation to an individual when:

- advice has been given to a responsible entity by the Secretary about a background check of the individual under section 21DA or 21DD, and
- after receiving the advice, the responsible entity makes a decision to grant, or continue to grant, the individual access to a critical infrastructure asset declared by the Minister, by notifiable instrument, for the purposes of paragraph 21ZB(2)(b), and
- during the period of 2 years beginning on the day the Secretary gives the advice, the

individual is convicted of, and sentenced to any term of imprisonment for, a *CIRMP level 2 offence* (set out in the table at clause 2 of Schedule 2, see Item 27 below), and

- the individual does not tell the Secretary in writing, within 7 days after individual is sentenced, the individual's name, date of birth and residential address, the date the individual was convicted and the court in which the individual was convicted and sentenced.

The offence in new subsection 21ZB(2) carries a penalty of 5 penalty units for failure to comply with the obligation within the 7 day timeframe. New paragraph 21ZB(2)(b) makes clear that the offence in subsection (2) does not apply if after a background check under section 21DA or 21DD the individual was not granted access, or did not continued to be granted access, to a critical infrastructure asset declared by the Minister for the purposes of paragraph 21ZB(1)(b).

The maximum penalty, expressly authorised by paragraph 18(2)(c) of the AusCheck Act, that could be imposed on an individual for a contravention of section 21ZB offence would be 5 penalty units, which is within the 50 penalty unit threshold for offences prescribed in regulations, as outlined at paragraph 3.3 of the Guide.

The primary purpose of the 5 penalty unit penalties being imposed on an individual by subsections 21ZB(1) and (2) is to recognise a potential hazard for a critical infrastructure asset or its operations. The penalties also recognise the possible risks of disruption, damage or danger to the security of a critical infrastructure asset posed by an individual who has been convicted of, or sentenced to a term of imprisonment in relation to, one of the serious and egregious *CIRMP level 1 or level 2 offences* after their background check has been conducted.

The intention of imposing a penalty for a failure to inform the Secretary of certain convictions and sentences to terms of imprisonment within the specified timeframes in section 21BA is to ensure that an individual is generally encouraged to comply with those obligations.

Item 25 – At the end of paragraph 26(a)

Section 26 of the AusCheck Regulations provides that individuals can apply to the Administrative Appeals Tribunal for review of decisions of the Secretary under provisions of specified in section 26.

Prior to the commencement of the Amendment Regulations, paragraph 26(a) provided that a decision of the Secretary to refuse to grant to an exemption in relation to an individual under subsection 5A(6) is reviewable by the Administrative Appeals Tribunal.

Item 25 would amend paragraph 26(a) of the AusCheck Regulations to provide that Administrative Appeals Tribunal Review also applies to decisions of the Secretary to refuse to grant an exemption under paragraph 21X(7).

The purpose and effect of this amendment is to make Administrative Appeals Tribunal review available to an individual who is provided notice by AusCheck that they have an unfavourable criminal history or are refused an exemption from specified identity verification requirements under subsection 21X(7).

The triggering of review mechanisms is important because a conviction for an offence specified in Schedule 2 to the AusCheck Regulations (see Item 27 below) may mean a person is assessed by a relevant responsible entity as not suitable to have unescorted access to its critical infrastructure asset.

It is important to note that seeking review of an adverse or qualified security assessment is not dealt with by section 26 of the AusCheck Regulations as that is not a decision made by the Secretary under the AusCheck Act or Regulations.

A review mechanism for an adverse or qualified security assessment is provided by subsection 27AA(1) of the *Administrative Appeals Tribunal Act 1975*, which states that an application under subsection 54(1) of the *Australian Security Intelligence Organisation Act 1979* for review of a security assessment may be made by a person in respect of whom the assessment was made and who has, in accordance with Part IV of that Act, been given notice of the assessment.

Item 26 – Paragraphs 30(3)(a) and (b)

Item 26 repeals and replaces subsection 30(3) of the AusCheck Regulations. In effect, this amendment expands the existing listed entities that may be liable to pay a fee (or if not paid, be liable for a debt due to the Commonwealth), if the discretion to charge a fee under subsection 30(1) or (2A) is exercised.

This is achieved by providing in subsection 30(3) that if a fee is payable under subsection 30(1) or (2A) by an individual or an issuing body, NHS entity, organising body or responsible entity that is not the Commonwealth or an unincorporated Commonwealth authority, the fee is a debt due to the Commonwealth and is recoverable by the Secretary on behalf of the Commonwealth.

This amendment will permit fees to be charged by AusCheck to an individual or to a responsible entity that is not the Commonwealth or an unincorporated Commonwealth authority for the conduct of background checks under the AusCheck scheme.

Item 27 – At the end of this instrument

Item 27 inserts new Schedule 2 into the AusCheck Regulations, which describes *CIRM program-security-relevant offences,* which are the offences that are defined to be a *CIRMP level 1 offence* and a *CIRMP level 2 offence* in clauses 1 and 2 respectively.

Item 1 of new Schedule 2 to the AusCheck Regulations prescribes the offences that are a *CIRMP level 1 offence* for the purpose of the definition of that term in subsection 4 of the

AusCheck Regulations. The offences prescribed by the table in Item 1 are offences involving or relating to:

- a weapon of mass destruction (item 1.1) or terrorism (item 1.2),
- treason, espionage or the disclosure of national secrets (item 1.3),
- engagement in hostile activities in a foreign country or involvement with foreign armed forces (item 1.4),
- the hijacking or destruction of an aircraft, vessel or offshore facility (item 1.5),
- the endangerment of an aircraft, airport, vessel, port or offshore facility that is used in commerce or owned by the Commonwealth or a State or Territory (item 1.6),
- an act of piracy at sea (item 1.7),
- slavery, or smuggling or trafficking of people (item 1.8) or a crime against humanity (item 1.9),
- murder, manslaughter or a threat to kill (item 1.10),
- assault, including indecent assault, sexual assault and sexual abuse (item 1.11),
- firearms, ammunition, weapons including the use of an item as a weapon, explosives or explosive devices or microbial or other biological agents or toxins (item 1.12),
- destruction of, or damage to, property or arson (item 1.13) and affray, riot or public violence (item 1.14),
- false imprisonment, deprivation of liberty, kidnapping or taking a hostage (item 1.15),
- participation in, or association with, serious and organised crime or gangs (item 1.16),
- the exploitation of a child (item 1.17), and
- robbery (item 1.19).

The intention of using 'national secrets' as an undefined term in item 1.3 provides for flexibility in the interpretation of this item to include, but not be limited to, the offences concerning the disclosure of information that would cause harm to Australia's interests under Part 5.6 of the *Criminal Code*.

Given that the offences defined as an *CIRMP level 1 offence* in Regulations are of a serious and egregious nature, and that certain individuals at critical infrastructure assets may be in security sensitive roles (including, for example, security screening staff or staff in a critical operational area), it is important for the responsible entity to have the capacity to review

relevant conviction information, with the individual's express consent for that information to be disclosed. If a person is convicted of any of the offences in Item 1 then the relevant responsible entity may consider advice about the conviction when making an assessment of the person with respect to suitability to have unescorted access to the responsible entity's critical infrastructure asset.

Item 2 of new Schedule 2 to the AusCheck Regulations prescribes the offences that are a *CIRMP level 2 offence* for the purpose of the definition of that term. The offences prescribed by Item 2 include offences involving or relating to:

- fraud, forgery, false identity or false identity documents (item 2.1),
- perjury, perverting the course of justice and intimidation (item 2.2),
- the production, possession, supply, importation or export of an illegal drug or a controlled substance (item 2.3),
- racial hatred or vilification (item 2.4),
- money laundering, currency violations or dealing with proceeds of crime (item 2.5) or bribery, corruption, extortion, racketeering or blackmail (item 2.6)
- obstructing, hindering, resisting or impersonating a government official or a law-enforcement officer (item 2.7),
- use, access, modification or destruction of data or electronic communications (item 2.8),
- theft or burglary (item 2.9),
- the intentional endangerment of persons (not including an offence that is a *CIRMP level 1 offence*) (item 2.10), and
- illegal importation or export of goods, fauna or flora or interference with goods under customs control (item 2.11).

As above in relation to *CIRMP level 1 offences* it is important for a responsible entity to have the capacity to review relevant *CIRMP level 2 offence* conviction, and sentencing, information, again with the individual's express consent for that information to be disclosed. If a person is convicted of, and is sentenced to a term of imprisonment for, any of the offences in Item 2 then the relevant responsible entity may consider advice about the conviction and sentence when making an assessment of the person with respect to suitability to have unescorted access to the responsible entity's critical infrastructure asset.

ATTACHMENT B

Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*

AusCheck Legislation Amendment (Critical Infrastructure Background Check) Regulations 2023

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

Overview of the Disallowable Legislative Instrument

The *AusCheck Act 2007* (the AusCheck Act) was amended by the *Security Legislation Amendment (Critical Infrastructure Protection Act)* 2022 (SLACIP Act) to enable AusCheck to conduct and coordinate background checks of an individual where a critical infrastructure risk management program (CIRMP) under the *Security of Critical Infrastructure Act 2018* (SOCI Act) permits a background check of an individual under the AusCheck scheme.

The SLACIP Act also amended the SOCI Act to include Part 2A, requiring certain responsible entities for critical infrastructure assets to adopt, maintain and comply with a CIRMP.

Under Part 7 of the SOCI Act, the Minister for Home Affairs may make rules for the purpose of paragraph 30AH(1)(c) and subsection 30AH(4) of the SOCI Act. The *Security of Critical Infrastructure (Critical Infrastructure risk management program) Rules (LIN 23/006) 2023* (the RMP Rules) will 'switch on' the Part 2A obligations, including the requirement to have a CIRMP. A CIRMP may permit AusCheck background checking to be conducted on an individual (referred to as 'a critical infrastructure background check').

A responsible entity under the SOCI Act for a critical infrastructure asset will be required to establish, maintain and comply with a CIRMP if the asset is of a type specified in rules. The purpose of this Disallowable Legislative Instrument is to set out the framework for conducting a background check under a CIRMP.

Whilst the AusCheck Act permits the conduct and coordination of the background check, the *AusCheck Regulations 2017* (AusCheck Regulations) set out the details of the AusCheck scheme. This Disallowable Legislative Instrument amends the AusCheck Regulations to provide a framework for critical infrastructure background checking and specify the criteria against which a critical infrastructure background check will be conducted.

This Disallowable Legislative Instrument amends the AusCheck Regulations to:

- introduce an authority for AusCheck to undertake background checks if a critical infrastructure background check of the individual is permitted under a CIRMP, and to conduct a further background check if there is a reasonable suspicion that the information provided for an initial background check was incomplete or the application requirements were not met;

- establish the components of an critical infrastructure background check, namely an identity verification check, an Australian criminal history check, a security assessment check and a migration status and right to work check;

- specify the information required to be included in an application for an critical infrastructure background check and other critical infrastructure background check application requirements;

- define terms for the purposes of a critical infrastructure background check;

- make provision for a background check advice to be issued to the individual and the responsible entity in relation after the background check has been conducted,

- expand the requirements that must be met to conduct electronic identity verification and in-person identity verification if required as part of a critical infrastructure background check;

- authorise the Secretary of Home Affairs (the Secretary) to grant an exemption from specified requirements of an electronic or in-person identity verification check if the individual is unable to meet those requirements;

- require the Secretary to give the individual written notice of, and reasons for, the preliminary assessment given by AusCheck if the individual has an unfavourable criminal history and enable the individual to make representations;

- require the Secretary to advise the responsible entity of the outcome of a background check of an individual;

- authorise the Secretary to request an individual or responsible entity do a specified thing to ensure information is provided and application requirements are met, and to cancel a background check where that request is not complied with;

- require the Secretary to give further advice about a critical infrastructure background check if the Secretary becomes aware that the initial advice is inaccurate or incomplete;

- impose an obligation on a responsible entity to inform the Secretary of certain decisions made in relation to granting access to the critical infrastructure asset or the revocation of access to the critical infrastructure asset, and create offences for failure to satisfy those obligations;

- include amendments to the basis on which a person can seek review of certain AusCheck decisions at the Administrative Appeals Tribunal (AAT). The amendments:
    - allow for review of decisions of the Secretary to refuse to grant an exemption to provide non-electronic identity documents; and
    - amend the definition of 'unfavourable criminal history' to include 'CIRMP criminal history' to allow for the review of a decision by the Secretary to advise that an individual has an unfavourable criminal history,
- authorise the Secretary to charge a fee for an application for an critical infrastructure background check, and
- setting out offences that are CIRMP-security-relevant offences in Schedule 2.

These amendments will enable AusCheck to contribute to the security and resilience of Australia's essential services, the economy, and national security by conducting background checks for responsible entities, to assist them with addressing specific risks to critical infrastructure that may be posed by personnel.

Different components of a critical infrastructure background check may be enlivened for different assets depending on the relevant responsible entity's CIRMP. The possible components to be enlivened for a critical infrastructure background check are an identity verification check (involving electronic and/or in-person identity verification), an Australian criminal history check, a security assessment (conducted by the Australian Security Intelligence Organisation in accordance with the *Australian Security Intelligence Organization Act 1979*) and a migration status/work entitlements check. If the CIRMP permits a security assessment to be conducted, the application is required to include details of how the CIRMP would manage an adverse security assessment or a qualified security assessment.

The outcomes of an AusCheck background check may lead to an assessment by a responsible entity that the individual poses a security risk to the critical infrastructure asset. Depending on the level of risk, the responsible entity may discontinue the individual's employment, move the individual to an area of the business where they are not able to access the critical infrastructure asset or may limit unescorted access to the critical infrastructure asset.

Personal information collected under the AusCheck scheme may be disclosed to law enforcement and national security authorities in response to a security incident. The retention and subsequent use and disclosure of AusCheck scheme personal information authorised under the AusCheck Act aims to assist law enforcement and national security agencies to respond to security incidents and perform their functions, including those that relate to the components of the background check performed by those agencies. Protections for the use

and disclosure of personal information and AusCheck scheme personal information are provided by both the *Privacy Act 1988* and the AusCheck Act, respectively.

Human rights implications

This Disallowable Legislative Instrument engages the following rights:

- Right to equality and non-discrimination – Article 2(1) and Article 26 of the *International Covenant on Civil and Political Rights* (ICCPR), Article 2(2) of the *International Covenant on Economic, Social and Cultural Rights* (ICESCR)

- Right to privacy– Article 17(1) of the ICCPR and Article 17 of the *Convention on the Rights of the Child* (CRC)

  Right to work– Article 6(1) of the ICESCR

Rights to equality and non-discrimination

Article 2(1) of the ICCPR and Article 2(2) of the ICESCR provide that the rights in both covenants are to be exercised without discrimination of any kind as to race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Similarly, Article 26 of the ICCPR provides that the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

The differential treatment of individuals by responsible entities on the basis of an AusCheck background check engages the rights of equality and non-discrimination on the basis of 'other status' (an individual's criminal or national security history). The amendments insert Subdivision D into Division 5 of the AusCheck Regulations to allow AusCheck to give advice to responsible entities about critical infrastructure background checks of individuals including an assessment of an individual's criminal history information. AusCheck will assess the individual's criminal history information against CIRMP-security-relevant offences. CIRMP-security-relevant offences are set out in Schedule 2 of the Disallowable Legislative Instrument.

The objective of this assessment is to identify individuals who have been convicted of CIRMP-security-relevant offences, which indicates that the individual may be a threat or risk to national security, which increases the likelihood or risk that the individual may cause harm at a critical infrastructure asset, which may also have a cascading effect on interdependent critical infrastructure assets. This element of the critical infrastructure background check informs the responsible entity's risk management decisions as outlined in their CIRMP.

The limitation on the rights to equality and non-discrimination that comes from a responsible entity taking action in response to AusCheck advice about an individual's background check is reasonable, necessary and proportionate. Firstly, actions taken in response to a background

checks do not apply to all individuals with a criminal history. Distinctions made on the basis of criminal history are only necessary for individuals who have CIRMP-security-relevant offences that appear in their criminal history. This is the least restrictive means of ensuring that individuals with access to critical infrastructure assets do not pose a threat to the security, or operability, of a critical infrastructure asset.

Further, a responsible entity does not have a mandatory obligation to take action in response to advice given by AusCheck. Rather, the responsible entity will need to take action in accordance with its CIRMP. This may include ensuring that the individual does not have unescorted access to a critical infrastructure asset, transferring an individual with an identified security risk to the critical infrastructure asset to another part of the business, or terminating the employment of an individual deemed to be too significant a risk to the critical infrastructure asset. To the extent that any action limits the right to freedom from discrimination, including freedom from discrimination in the exercise of work rights, discussed below, any limitation is reasonable and necessary. The impact of security hazards to critical infrastructure assets has the potential to significantly disrupt that infrastructure. It is reasonable and necessary to ensure that personnel risks to those assets are adequately identified and managed, to protect national security and public order.

Appropriate safeguards also exist if an individual is issued with an 'unfavourable criminal history'. Section 26 of the AusCheck Regulations provides that a person can seek AAT review of a decision by the Secretary to advise that an individual has an 'unfavourable criminal history'. The Disallowable Legislative Instrument will amend the definition of 'unfavourable criminal history' to include 'CIRMP criminal history' meaning that a person will be able to seek AAT review of advice that the outcome of an AusCheck background check is that they have been found to have an 'unfavourable criminal history'. This ensures that to the extent the measures limit the right to non-discrimination, any limitation is not arbitrary, and is reasonable and proportionate.

Right to privacy

Article 17(1) of the ICCPR provides that no one shall be subjected to arbitrary or unlawful interference with their privacy. The Disallowable Legislative Instrument will engage the right to privacy by enabling the collection, use, storage and disclosure of personal information for the purposes of conducting a critical infrastructure background check.

The right to privacy is engaged where AusCheck conducts a background check under sections 11AD or 11AE of the Disallowable Legislative Instrument. Under section 11AE, AusCheck can undertake a background check if permitted by a CIRMP and application has been made by the individual. An individual must then provide information required under section 5 of the AusCheck Regulations, which includes additional information relating to the capacity in which the individual is employed and reasons why a background check is permitted under the CIRMP. Personal information is provided voluntarily by an individual with their express consent to it being used for a background check. An individual will be provided with a privacy notice by AusCheck detailing how their information will be used to

ensure consent is fully informed. AusCheck has updated the privacy notice to capture the amendments in this instrument. Section 29 of the AusCheck Regulations allows the Secretary to issue guidelines about the use and disclosure of information in the AusCheck database. The guidelines are currently publically available on the Department's website. All AusCheck staff members are required to comply with the guidelines, and section 15 of the AusCheck Act also provides an offence provision for AusCheck staff members who unlawfully disclose AusCheck scheme personal information. To the extent that the right to privacy is limited by an individual's disclosure of their personal information for the purposes of a background check, the limitation is reasonable, necessary and proportionate to achieve the legitimate objective of assisting responsible entities to identify and manage personnel risks to critical infrastructure assets.

Under section 11AE of the Disallowable Legislative Instrument, AusCheck may undertake a further background check if, after the original background check, the Secretary considers on reasonable grounds that the individual has a CIRMP criminal record or constitutes a threat to the security of an asset of a kind declared by the Minister by notifiable instrument. It is reasonable to expect that if someone, since the last background check, commits a CRIMP-security-relevant-offence or constitutes a threat to the security of the critical infrastructure asset, a further background check be conducted to allow the responsible entity assess the suitability of the individual to have continued access their asset and manage any risks arising from the commission of a CIRMP-security-relevant-offence.

To the extent that section 11AE limits the right to privacy, this limitation is permissible as the collection of personal information would be lawful, would not be arbitrary and would be reasonable, necessary and proportionate to achieving a legitimate national security objective.

The right to privacy is also engaged where AusCheck provides advice to the responsible entity under section 21DA of the Disallowable Legislative Instrument about whether or not an individual has an unfavourable criminal history (including further detail about the offence), or whether a security assessment of the individual is an adverse security assessment or qualified security assessment.

These measures also engage the right to privacy under Article 16 of the CRC. This Article provides that no child shall be subjected to arbitrary or unlawful interference with their privacy. The measures in the Disallowable Legislative Instrument will enable the collection, use and disclosure of the personal information of a person under the age of 18, for the purposes of a critical infrastructure background check. Enabling a responsible entity to conduct a background check on a person under 18 is a reasonable and necessary measure. Some critical infrastructure assets, for example critical food and grocery assets, engage a significant number of employees under 18. It may be necessary in some instances for responsible entities to include background checks as a condition of employment in relation to certain critical assets (for example, food distribution centres). However, the measures are proportionate and contain appropriate safeguards. . The amendments will insert a provision that requires the express consent of a parent or guardian to a background check where the individual is under the age of 16 at the time of the application.

The purpose of collecting, using, storing and disclosing information to conduct background checks is reasonable and necessary for the purpose of identifying and mitigating against personnel hazards to critical infrastructure assets and the essential services delivered by them. This is achieved by using an individual's personal information, to conduct a background check to identify whether they would constitute a threat to secure areas, systems, processes or people. This information is then disclosed to the responsible entity so that the entity can consider any risk posed by the individual within the context of their CIRMP.

Appropriate safeguards exist to ensure that use of an individual's personal information is reasonable and proportionate. While a responsible entity will receive advice from AusCheck that an individual has an 'unfavourable criminal history', under paragraph 21DA(5)(c) of the Disallowable Legislative Instrument, a responsible entity can only be provided with details of the CIRMP offence if the individual provides express consent for the details to be provided. Protections for the use and disclosure of personal information and AusCheck scheme personal information are provided by both the *Privacy Act 1988* and the AusCheck Act, respectively. To the extent that privacy is limited by the measures in the Disallowable Legislative Instrument, the limitation is reasonable, necessary and proportionate in achieving the legitimate objective of protecting critical infrastructure assets.

Right to work

Article 6(1) of the ICESCR provides for the right to work, including the right of everyone to the opportunity to gain a living by work which the persons freely chooses or accepts. The right to work does not equate to a guarantee to particular employment. The United Nations Committee on Economic Social and Cultural Rights has stated that this protection includes the right to not be unfairly deprived of work. Any limitations need to be reasonable, necessary and proportionate to the legitimate objective sought to be achieved.

The outcome of an AusCheck critical infrastructure background check may lead to an assessment by a responsible entity to take a number of actions, including terminating a person's employment if the person has been convicted of a CIRMP level 1 offence or convicted of and sentenced to imprisonment for a CIRMP level 2 offence. Undergoing a critical infrastructure background check may be an essential requirement for people who work at a critical infrastructure asset, for example, people who work in, at or in connection with a critical component of a critical infrastructure asset or those who manage the security measures of that component. Therefore AusCheck's advice could limit the right to work of some individuals, particularly if an individual has been convicted of a CIRMP level 1 offence, or convicted of and sentenced to imprisonment for a CIRMP level 2 offence, or where an adverse or qualified security assessment has been made in respect of the individual, if the result of advice from AusCheck is that the responsible entity considers the individual to be too significant a risk to the critical asset and terminates the person's employment.

To the extent that these provisions may limit the right to work in relation to a critical infrastructure asset, the limitation is reasonable if the risk is of such significance that it would be reasonable to expect the responsible entity to mitigate the risk. A responsible entity needs

to be able to appropriately manage and mitigate those risks for their critical infrastructure asset. To the extent that the right to work is engaged, any limitation is reasonable and proportionate. Limiting or controlling access to a critical infrastructure asset or a critical component of one only affects the person's access to that critical infrastructure asset and may not impact their ability to be employed within other areas of the business or the sector.

The potential limitation of the right to work is reasonable and necessary because it applies to CIRMP-security-related-offences, which are offences that have the greatest risk to critical infrastructure assets. . Given the risks associated with damage to, or destruction of a component of a critical infrastructure asset or the disruption or cessation of the essential service provided by a critical infrastructure asset, it is reasonable to conduct background checks on individuals who may seek to work at a critical infrastructure asset, even where those background checks may result in the responsible entity terminating a person's employment. This reflects the serious nature of those offences and of the risks to security that a person with such a conviction, or who is the subject of such a security assessment, may pose to the critical infrastructure asset in question. Therefore any limitation is considered to be reasonable and necessary to achieve the legitimate objective of protecting national security and public order.

It is also noted that nothing in the instrument, AusCheck Act or SOCI Act truncates or limits the rights of employees under the *Fair Work Act 1999* or relevant State or Territory industrial relations legislation. Responsible entities will still need to comply with all requirements concerning dismissal or redundancy under that legislation.

Conclusion

The Disallowable Legislation Instrument is compatible with human rights because to the extent that it may limit human rights, those limitations are reasonable, necessary and proportionate.

The Honourable Clare O'Neil MP

Minister for Home Affairs