CONSULTATION DRAFT v2

AusCheck Background Checks for the purpose of a Risk Management Program

As at 24 October 2022

This paper is being released together with the draft *Security of Critical Infrastructure (Critical infrastructure Risk Management Program) Rules 2022* (draft RMP Rules) to aid in interpretation and understanding of proposed section 9 of the draft RMP Rules, which have been released for consultation in accordance with section 30AL of the *Security of Critical Infrastructure Act 2018*.

The *AusCheck Regulations 2017* (AusCheck Regulations) will need to be amended to facilitate these background checks. The amendments to the AusCheck Regulations will facilitate the conduct of background checks as set out in this discussion paper, after consideration of feedback received during consultation on the draft RMP Rules.

Contents

Overview 1
1. Background 3
How do the draft RMP Rules allow for background checks? 3
2. Background checks of 'critical workers' may be used to minimise personnel hazards 4
Requirements that apply for naval shipbuilding 5
3. What will a background check involve? 5
4. The background check process 5
Step 1: Responsible entity identifies critical workers 6
Step 2: Applying for a background check 7
Step 3: Identify verification 7
Step 4: Completion of further components of the background check 8
Step 5: Advice about the outcome of the background check 10
Step 6: Responsible entity makes a suitability decision 10

Overview

The draft *Security of Critical Infrastructure (Critical infrastructure Risk Management Program) Rules 2022* (draft RMP Rules), proposed to be made by the Minister for Home Affairs under the *Security of Critical Infrastructure Act 2018* (SOCI Act), provide for the conduct of background checks of critical workers by AusCheck.

A background check is not required to be conducted, but is a tool that can be used by responsible entities as part of their approach to minimising personnel risks to the operation of their critical infrastructure asset(s) to minimise personnel risks.

The proposed components of such a background check are:

(a) an electronic and in-person identity check

(b) a criminal history check conducted by the Australian Criminal Intelligence Assessment (ACIC)—to assist AusCheck to determine whether a critical worker has met the criminal history criteria

(c) a security assessment conducted by the Australian Security Intelligence Organisation (ASIO), and

(d) if the identity check does not establish that the critical worker is an Australian citizen—a right to work check conducted via the Visa Entitlement Verification Online system (VEVO).

The process of conducting background checks would involve:

Step 1: Identification	Responsible entity for a critical infrastructure asset identifies their critical workers via an online portal established by AusCheck.
Step 2: Application	Responsible entity or critical worker applies to AusCheck for a background check.
Step 3: Identity verification	Electronic and in-person identity check conducted by checking partners, e.g. Australia Post.
Step 4: Further components completed	AusCheck arranges for ACIC, ASIO and VEVO checks to be completed, and makes assessment about whether the worker has met the criminal history criteria.
Step 5: Advice about the outcome	AusCheck, via its online portal, advises critical worker and responsible entity of the outcome of the background check.
Step 6: Suitability decision	Responsible entity makes decision on the suitability of the critical worker to have access to the critical components of their critical infrastructure asset(s).

This paper sets out further detail in relation to each step for you to consider in making any submission to the Minister for Home Affairs on the draft RMP Rules.

1. Background

1.1. Under the draft RMP Rules, responsible entities for certain critical infrastructure assets are being asked to adopt, maintain and comply with a critical infrastructure risk management program (RMP) under Part 2A of the SOCI Act.

1.2. It is currently proposed that the RMP obligations in Part 2A will be applied to responsible entities for the following critical infrastructure assets as defined by the SOCI Act (see section 5 of the SOCI Act, Part 1, Section 4 of the draft RMP Rules):

critical broadcasting assets	critical gas assets	critical liquid fuel assets
critical domain name systems	critical hospitals[1]	critical financial market infrastructure assets that are ***payment systems*** (as defined by the *Payment Systems (Regulation) Act 1998*)
critical data storage or processing assets	critical food and grocery assets	
critical energy market operator assets	critical freight infrastructure assets	critical water assets
critical electricity assets	critical freight services assets	

How do the draft RMP Rules allow for background checks?

1.3. Subsection 30AH(1) of the SOCI Act sets out that an RMP is a written document, or collection of documents, that a responsible entity adopts for their critical infrastructure asset(s) which:

(a) must identify:

- hazards for which there is a material risk that the hazard could have a **relevant impact** on the asset[2]
- reasonable steps to mitigate or eliminate the material risk of the hazard occurring, and
- reasonable steps to mitigate the impact if the hazard occurs, and

(b) must meet the requirements specified in rules by the Minister for Home Affairs.

1.4. Subsection 30AH(4) provides that the rules made under paragraph 30AH(1)(c) may require that an RMP include one or more provisions that permit a background check to be conducted under the AusCheck scheme.

[1] Only select hospitals will be included—this is subject to ongoing consultation with relevant stakeholders (see also Schedule 2 of the draft RMP Rules).
[2] See definition of 'relevant impact' in subsection 8G(1) of the SOCI Act.

1.5. The Minister for Home Affairs is required to consult on rules made under paragraph 30AH(1)(c) before the rules can be made. The draft RMP Rules have been released for this purpose.

1.6. The draft RMP Rules set out general governance requirements (Part 2, Section 7) as well as specific requirements in relation to:

(a) cyber and information security hazards (Part 2, Section 8)

(b) personnel hazards (Part 2, Section 9)

(c) supply chain hazards (Part 2, Section 10), and

(d) physical security hazards and natural hazards (Part 2, Section 11).

2. Background checks of 'critical workers' may be used to minimise personnel hazards

2.1. Under section Part 2, Section 9 of the draft RMP Rules, responsible entities will be required to identify their **critical workers** and assess the suitability of those workers to have access to **critical components** of their critical infrastructure asset(s). To make this assessment, the responsible entity **may** require critical workers to undergo background checks under the AusCheck scheme, or via an alternative process or system set out in their RMP.

2.2. The terms **critical worker** and **critical component** are defined in section 5 of the SOCI Act and cannot be amended without an Act of the Commonwealth Parliament.

2.3. A **critical worker** is defined to be an individual:

(a) who is an employee, intern, contractor or subcontractor of a responsible entity

(b) whose absence or compromise would prevent the proper functioning of the responsible entity's critical infrastructure asset, or cause significant damage to the asset, and

(c) who has access to, or control and management of, a critical component of the asset.

2.4. An individual must meet all three of the requirements set out in paragraphs (a), (b) and (c) above to be a critical worker.

2.5. A **critical component** of a critical infrastructure asset is defined as a part of the asset where, in the assessment of the responsible entity, the absence, damage or compromise of that part of the asset would either:

(a) prevent the proper functioning of the asset, or

(b) cause significant damage to the asset.

2.6. One way that a responsible entity will be able to assess the suitability of critical workers to have access to critical components of their critical infrastructure asset(s) is to have a background check under the AusCheck scheme conducted at regular

intervals as determined by the Responsible Entity. (see Part 2, Section 9 of the draft RMP Rule).

2.7. **To be absolutely clear, the draft RMP Rules do NOT require all critical workers to be subject to an AusCheck background check.** The draft RMP Rules provide for the conduct of background checks if the responsible entity wishes to use these to minimise personnel hazards to their critical infrastructure asset(s).

Requirements that apply for naval shipbuilding

2.8. The exception to paragraph 2.7 above is in relation to draft *Security of Critical Infrastructure (Naval shipbuilding) Rules 2022* (draft Naval Shipbuilding Rules).[3]

2.9. The draft Naval Shipbuilding Rules will require the responsible entity for Osborne Naval Shipyard (ONS) to adopt, maintain and comply with procedures and processes by which any person who has unescorted access to ONS must have undergone a background check. This is a unique requirement that only applies for ONS under the draft Naval Shipbuilding Rules.

3. What will a background check involve?

3.1. Proposed section 9 of the draft RMP Rules sets out the proposed components of a background check for the purpose of an RMP. If the responsible entity elects to use background checks to minimise personnel security hazards, the components are all of the following:

(a) an electronic and in-person identity verification conducted by an identity verification partner, such as Australia Post, on behalf of AusCheck

(b) a criminal history check conducted by the Australian Criminal Intelligence Commission (ACIC), against which AusCheck assesses whether or not the critical worker has been the criminal history criteria set out in Schedule 1 to the draft RMP Rules

(c) a security assessment conducted by the Australian Security Intelligence Organisation (ASIO), and

(d) a right to work check conducted via the Visa Entitlement Verification Online system (VEVO)—if the identity check does not indicate that the person is an Australian citizen.

4. The background check process

4.1. If a responsible entity elects to use background checks to minimise personnel hazards, the proposed background check process under the draft RMP Rules and amended AusCheck Regulations will be:

(a) responsible entity identifies critical workers

[3] See further detail at: <Osborne Naval Shipyard Formal Consultation (auscheck.gov.au)>

(b) responsible entity or critical worker makes an application to conduct a background check of the worker

(c) verifying the identity of the critical worker

(d) completion of the other components of the background check

(e) advice from AusCheck to the responsible entity, critical worker and the workers employer (if different to the responsible entity) about the outcome of the background check, and

(f) the responsible entity making a suitability decision following advice from AusCheck about the outcome of the background check.

Step 1: Responsible entity identifies critical workers

4.2. The responsible entity who owns or operates a critical infrastructure asset to which Part 2A of the SOCI Act applies will be required to identify the critical workers for their critical infrastructure asset(s).

4.3. Once critical workers are identified, the responsible entity will need to apply the process or system outlined in their RMP to assess the suitability of their critical workers to have access to the critical components of their asset(s). One way in which suitability can be assessed is by requesting a background check to be conducted by AusCheck. There may be existing programs in place or another way to look at suitability that is more appropriate or specific to a critical infrastructure provider.

How long will it take to identify critical workers?

4.4. Under the draft RMP Rule, responsible entities will have six months after the rule is made to comply with the obligation to minimise personnel hazards. This includes requiring AusCheck background checks to be conducted if the entity elects to use these checks to minimise personnel risks.

4.5. It is suggested that responsible entities start identifying their critical workers as soon as possible, so that applications for background checks can start to be made once the draft RMP Rules are made.

What if a critical worker does not want to be background checked?

4.6. The legal obligation created by the draft RMP Rule is for the responsible entity to identify critical workers and to assess the suitability of those workers to have access to critical components of their asset(s).

4.7. The responsible entity will need to negotiate how it meets this obligation with its current employees and contractors. If a critical worker does not want to be background checked, and this is required by the responsible entity, the critical worker and responsible entity will need to negotiate an alternate outcome in accordance with the responsible entity's processes and systems, all other obligations under legislation and contractual agreements.

What if a critical worker is not background checked before the requirement applies to the responsible entity?

4.8. The Cyber and Infrastructure Security Centre has consistently indicated that the instigation of a RMP is a step change with initial compliance focused around education and awareness raising in the implementation of this change. The approach is outlined in the published *Cyber and Infrastructure Security Centre Compliance and Enforcement Strategy - April 2022.*

Step 2: Applying for a background check

4.9. Once critical workers are identified, the responsible entity or the individual critical worker will be able to apply to AusCheck for a background check. Applications will be made electronically via a portal that will be available on the AusCheck website.

4.10. If an application is made by the responsible entity on behalf of a critical worker, the application will need to include information that the responsible entity has obtained express, informed consent from the critical worker to request a background check on their behalf. A detailed privacy notice that sets out the matters required under the *Privacy Act 1988* will be provided at the time of making an application.

4.11. Where a background check of a critical worker has already been undertaken, the Secretary of the Department of Home Affairs (or the Secretary's delegate) may be able to request that a further background check be conducted.

Will there be a fee for applying for a background check?

4.12. Yes, a fee will be payable to assist with the processing of the background check.

Step 3: Identify verification

4.13. Once a complete application is received, the first action that will be taken is to verify the identity of the critical worker. This will involve both an electronic identity verification check and an in person identity verification check. You will be asked to supply at least 3 separate documents that are electronically verifiable through the Department of Home Affairs' Document Verification Service (DVS) to establish your identity before we can do a background check. The documents you need are:

(a) Category A—to evidence the start of your identity in Australia

(b) Category B—a government-issued identity document with your photograph and signature, and

(c) Category C—evidence of the use of your identity in the community.

4.14. Provide one document from each of categories A, B and C. You may also need to provide: a document that shows your current address – if no other document has your current residential address or documents to show a change of legal name. For example, an Australian birth certificate a current and valid driver licence, and a Medicare card could be sufficient to verify your identity. More information can be found on the AusCheck website.

What if a critical worker cannot provide the required identity documents?

4.15. If a critical worker cannot provide the required documents for an electronic or in person identity verification check, a process to request an exemption will be available.

4.16. If a request for an exemption is refused, or the critical worker cannot meet the alternate requirements in the exemption, merits review of the exemption decision will be available in the Administrative Appeals Tribunal.

4.17. If, after all exemptions and appeals are expired, the critical worker's identity cannot be verified, AusCheck will not be required to continue undertaking the background check. In these circumstances, advice will be provided to the critical worker and the responsible entity via the AusCheck online portal and the responsible entity will be required to make a decision on the critical worker's suitability (see Step Six below).

Step 4: Completion of further components of the background check

4.18. Once a critical worker's identity has been verified, AusCheck will arrange for the further three components of the background check to be completed.

(a) A criminal history check will be completed by the ACIC.

(b) A security assessment by ASIO.

(c) If the critical worker has not been identified as an Australian citizen—a right to work check from VEVO.

4.19. These are the only components that will be included in a background check by AusCheck. A background check **does not** include additional checks such as a review of a critical worker's internet browsing history by AusCheck.

(a) Criminal history check

4.20. AusCheck will seek criminal history information from the ACIC.

4.21. Once input is received from the ACIC by AusCheck, AusCheck will make an assessment about whether or not the critical worker meets the **criminal history criteria**. As set out in the draft RMP Rule, a critical worker will not meet the criminal history criteria when:

(a) the worker has been convicted of an offence mentioned in the following table (see clause 1 of Schedule 1), or

relating to weapons of mass destruction or terrorism	piracy, treason, espionage or disclosure of national secrets
engaging in foreign hostilities and with foreign armed forces	hijacking or destruction of aircraft, vessels or offshore facilities
endangerment of an aircraft, airport, vessel, port or offshore facility	slavery or people smuggling
murder, manslaughter or threat to kill	indecent or sexual assault, exploitation of a child

offences involving firearms, ammunition, weapons, explosives and biological agents	destruction or damage to property, including arson
relating to association/participation with serious and organised crime or gangs	false imprisonment, kidnapping or hostage taking
robbery	affray, riot or public violence

(b) the worker has been convicted of, and sentenced to imprisonment for, an offence mentioned in the following table (see clause 2 of Schedule 1).

production, possession, supply, importation or exportation of an illegal drug or other controlled substance	perjury, intimidation or perverting the course of justice
racial hatred or vilification	fraud or forgery
money laundering, currency violations or dealing with the proceeds of crime	bribery, corruption, extortion, racketeering or blackmail
hindering, resisting or impersonating a government official or law enforcement officer	use, access, modification or destruction of data or electronic communications
theft or burglary	intentional endangerment of persons not specified elsewhere
illegal import or export of goods, fauna or flora	interference with goods under customs control

4.22. The criminal history criteria will apply generally for critical workers in all critical infrastructure sectors.

4.23. In giving consideration to whether a critical worker has not met the criminal history criteria, AusCheck will be able to request a critical worker provide more information in accordance with the process set out in section 11A of the AusCheck Regulations.

Criminal history check: preliminary assessment that the critical worker has an 'unfavourable criminal history'

4.24. If AusCheck assesses that a critical worker has not met the criminal history criteria, they will be required to notify the worker in writing that they have made a preliminary assessment that the individual has an unfavourable criminal history—setting out the assessment made and the reasons for the assessment.

4.25. A critical worker who receives notice of a preliminary assessment will have the opportunity to respond to the contents of the assessment by the day set out in the notice within 28 days, and request further time to respond if necessary. AusCheck will not be able to provide advice about the outcome of the background check (see Step 5) until a response is received or the timeframe to provide a response is expired.

4.26. If, after all of the processes above are completed, the critical worker continues to disagree with AusCheck's preliminary assessment the worker will have the ability to apply to the Administrative Appeals Tribunal for review.

Criminal history check: how does the spent convictions scheme apply?

4.27. In certain circumstances, a critical worker cannot be required to disclose that they have been charged with or convicted of an offence and AusCheck cannot take the offence into account when assessing whether the worker has met the criminal history criteria. This occurs where:

(a) the critical worker was pardoned, not sentenced to imprisonment, or sentenced to less than 30 months imprisonment, for the offence

(b) the worker has not been convicted of another offence in the 10 years after their conviction (or 5 years if convicted as a child), and

(c) an exclusion does not apply.

(b) Security assessment

4.28. ASIO is responsible for the security-checking component—the CISC requests thousands of security assessments from ASIO each year to support AusCheck's conduct and coordination of background checks of individuals. The conduct of a security assessment is subject to the legislative regime outlined in the *Australian Security Intelligence Organisation Act 1979.*

4.29. If a critical worker has an adverse security assessment or qualified security assessment from ASIO, the critical worker will be able to appeal the merits of the assessment to the Administrative Arrangement Tribunal.

(c) Right to work check

4.30. A Visa Entitlement Verification Online (VEVO) check protects against employing people who are not legally entitled to work in Australia. A VEVO report includes information on which visa an individual has and its expiry date, an individual's 'must not arrive after' date and the individual's period of stay and conditions.

Step 5: Advice about the outcome of the background check

4.31. Once all of the components of a background check have been completed, AusCheck will upload the following information to the electronic portal:

(a) whether the critical workers identity has been verified

(b) whether or not the worker meets the criminal history criteria

(c) the outcome of the ASIO security assessment, and

(d) if necessary—the outcome of the right to work check by VEVO.

What if a critical worker disagrees with the outcome of the background check?

4.32. Decisions made in the AusCheck scheme may be subject to review or appeal under the *Administrative Decisions (Judicial Review) Act 1997*, or in limited circumstances by the Administrative Appeals Tribunal.

Step 6: Responsible entity makes a suitability decision

4.33. After the responsible entity receives the outcome of the background check for the critical worker, the entity will be required under the RMP Rules to assess whether it

is suitable for the critical worker to have access to the critical components of the entity's critical infrastructure asset(s).

4.34. The outcome of this suitability decision could include mitigations such as access requirements or particular positions. How and when mitigations will be applied will be required to be set out in the responsible entity's RMP.

4.35. For example, a responsible entity's RMP may set out that a critical worker must not have unescorted access to critical components of their asset(s) as it presents a material risk of a personnel hazard occurring. The responsible entity will need to take action to mitigate the risk, which will also be set out in the RMP. The critical worker and responsible entity will need to negotiate how the mitigations apply to the worker in accordance with the responsible entity's processes and systems set out in the RMP, as well as all other obligations under legislation and contractual agreements.

4.36. **The SOCI Act and draft RMP Rules do not provide any defences or exceptions for the responsible entity from obligations that may apply under contract or employment laws. Nothing in the check abrogates responsibilities under the *Fair Work Act 2009* or other legislation.**

4.37. The responsible entity will need to negotiate how it will make suitability decisions after receiving advice about the outcome of a background check with its current and future employees and contractors.

Should you wish to discuss this paper in detail you can arrange a meeting on 1300 272 524 or email enquiries@CISC.gov.au