EXPLANATORY STATEMENT

Issued by authority of the Minister for Finance

Digital ID Act 2024

Digital ID (Accreditation) Amendment (PSPF and Other Measures) Rules 2025

Section 168 of the *Digital ID Act 2024* (Digital ID Act) provides that the Minister may, by legislative instrument, make rules prescribing matters required or permitted by the Digital ID Act to be prescribed by the rules, or necessary or convenient to be prescribed for carrying out or giving effect to the Digital ID Act.

The Digital ID Act establishes a legal framework for a secure and voluntary digital ID system in Australia, enabling individuals to verify their identity online when interacting with government and businesses, while regulating and accrediting service providers to ensure strong governance, security, and consumer protections.

The *Digital ID (Accreditation) Rules 2024* (the Rules) support the operation of the Digital ID Act which aims to provide individuals with secure, convenient, voluntary and inclusive ways to verify their identity for use in online transactions with government and businesses.

The *Digital ID (Accreditation) Amendment (PSPF and Other Measures) Rules 2025* (Amendment Rules) amends the Digital ID (Accreditation) Rules to enhance the functionality of the Australian Government Digital ID System. In particular, the Amendment Rules:

- provide a separate duration of express consent when given to an accredited Attribute Service Provider for a business purpose.
- incorporate the Protective Security Policy Framework (*PSPF*) by reference and to also limit the PSPF to Australian non-corporate Commonwealth entities, mandate alternative frameworks for others, and introduce a three-month transition period for future PSPF updates.
- extend by 12 months the implementation period for transitioned accredited entities to comply with digital ID voluntary suspension and resumption obligations.

Details of the Amendment Rules are set out in **Attachment A**.

The Amendment Rules are a legislative instrument for the purposes of the *Legislation Act 2003*.

The Amendment Rules commences on the day after the instrument is registered on the Federal Register of Legislation.

GLOSSARY

This Explanatory Statement uses the following abbreviations and acronyms.

Abbreviation	***Definition***
ASP	Attribute Service Provider
AGDIS	Australian Government Digital ID System
IP level	Identity proofing level
ISP	Identity Service Provider
NCEs	Non-corporate Commonwealth Entities
PSPF	Protective Security Policy Framework

ATTACHMENT A

Details of the *Digital ID (Accreditation) Amendment (PSPF and Other Measures) Rules 2025*

Section 1 – Name

1.1. The name of this instrument is the *Digital ID (Accreditation) Amendment (PSPF and Other Measures) Rules 2025* (Amendment Rules).

Section 2 – Commencement

1.2. This instrument commences the day after this instrument is registered on the Federal Register of Legislation.

Section 3 – Authority

1.3. This section provides that this instrument is made under section 168 of the *Digital ID Act 2024* (Digital ID Act).

1.4. Section 168 of the Digital ID Act enables the Minister to make legislative instruments, such as the Amendment Rules. The purpose of this section is to set out the authority under which this instrument is made.

Section 4 – Schedules

1.5. This section provides that each instrument that is specified in a Schedule to this instrument is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this instrument has effect according to its terms.

1.6. The purpose of this section is to provide for how the amendments in this instrument operate.

Schedule 1—PSPF amendments

Overview

1.7. This Schedule incorporates certain controls of the Protective Security Policy Framework (PSPF). The purpose of these amendments is to ensure the latest release of PSPF is applied in the Accreditation Scheme at the relevant time. These amendments are designed to enhance precision and alignment with the PSPF by the Accreditation Scheme, and consistency with the broader whole-of-government protective security policy framework.

1.8. The PSPF is owned and maintained by the Department of Home Affairs and sets out Australian Government's protective security policy across six security domains. The PSPF provides for what Australian Government entities must do to protect their people, information and resources, both domestically and internationally. The PSPF is published online and is freely available online at: https://www.protectivesecurity.gov.au.

1.9. The PSPF is subject to annual review to ensure that it continues to reflect current threats. The Department of Home Affairs consults with the relevant impacted bodies before changes are made to the PSPF. This ensures that impacted bodies are aware of the new upcoming changes and understand their compliance obligations.

1.10. The purpose of these amendments is to introduce several policy changes that support a more responsive protective security framework compliance model under the Accreditation Rules:

- Incorporation of PSPF by reference: Previously, relevant requirements within the PSPF were replicated in the Accreditation Rules. The PSPF is now incorporated by reference into the Amendment Rules. This change enables timely adoption of future PSPF updates, ensures alignment with whole-of-government protective security policy, improves regulatory responsiveness, and ensures that protective security obligations under the Accreditation Rules remain fit-for-purpose.

- Application to Non-Corporate Commonwealth Entities: In line with broader whole-of-government security frameworks, non-corporate Commonwealth Entities (NCE) must comply with the PSPF, consistent with their obligations under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) and broader Commonwealth whole-of-government security policies.

- Application period: A 3 month period is provided for entities to comply with any changes to the PSPF that occur after these amendments commence. This allows NCEs time to make changes to their digital ID systems or documents to comply with the PSPF, noting they are already required to comply with the PSPF under the PGPA Act.

- Alternative frameworks for other entities: Entities that are not NCEs may choose to comply with ISO/IEC 27001 or an alternative equivalent framework, if they can demonstrate compliance with all required controls under ISO/IEC 27001. This provides flexibility while maintaining regulatory assurance.

1.11. These rules now distinguish between a ***protective security framework*** and ***protective security framework controls***. This amendment improves the precision of the relevant

legislative provisions and reflects the policy of requiring entity to comply with specific controls, rather than implementing a framework as was previously the case.

Item 1 – Subrule 1.4(2)

1.12. This item inserts a new definition of ***non-corporate Commonwealth entity*** into subrule 1.4(2). The new definition adopts the same meaning as in the PGPA Act.

1.13. Under the PGPA Act, an NCE is a body that is a part of the Commonwealth. NCEs are accountable to Parliament and subject to the financial and corporate governance arrangements of the PGPA Act.

1.14. The purpose of this amendment is to distinguish NCEs from other types of accredited entities, particularly in relation to their protective security framework requirements. NCEs are required implement the PSPF, consistent with their obligations as Commonwealth entities.

Items 2 - 4 – Subrule 1.4(2) (definition of *protective security framework),* subrule 1.4(2), subrule 1.4(2) (note 1 and note 2 to the definition of the *PSPF*)

1.15. Items 2 to 4 of these Amendment Rules amend and introduce new definition terms relating to the protective security framework requirements within the Accreditation Rules. Collectively, the purpose of these changes is to clarify the scope and structure of protective security framework obligations. The amendments are also intended to assist in distinguishing between the protective security framework that applies to an entity and the individual protective security controls within each framework and align terminology to reflect a compliance-based approach. This approach provides greater certainty to accredited entities by clearly articulating their obligations and enabling more consistent implementation and assessment of protective security requirements.

1.16. Item 2 repeals and substitutes the definition of ***protective security framework***. Previously, the term was defined by reference to Division 2 of Part 4.1 of Chapter 4, which provides for the protective security frameworks in the Accreditation Rules. The revised definition now explicitly identifies three protective security frameworks in the Accreditation Rules, which are the PSPF, ISO/IEC 27001 or an alternative framework. This provides greater precision in the references to the relevant or specified controls in provisions across the Accreditation Rules.

1.17. Item 3 inserts a new definition of ***protective security framework control*** into subrule 1.4(2), which is defined to mean a relevant PSPF control, a control specified in ISO/IEC 27001 or a control specified in an alternative framework in rule 4.5. The purpose of this change is to create a clearer distinction between a “protective security framework” as a whole and the individual controls within a protective security framework.

1.18. This definition supports the revised structure in Chapter 4, which focuses on the introduction of specific protective security controls rather than the adoption of an entire protective security framework. To reflect this shift the language used in the Rules has also been refined, entities are now required to comply with individual controls, recognising that compliance with a framework is best achieved through meeting these relevant specific controls.

1.19. Item 4 repeals and substitutes the notes under the definition of *PSPF*.

1.20. New Note 1 under the definition of *PSPF* provides the web address for where the PSPF could be accessed in 2025.

1.21. The purpose of the new Note 1 is to assist the reader by providing for the web address where the PSPF could be accessed in 2025 and at the time of commencement.

1.22. The new Note 2 under the definition of PSPF clarifies that, at the time rule 1.7A commenced, the current version of the PSPF was the PSPF published on 24 July 2025.

1.23. The purpose of the new Note 2 is to clarify which version of the PSPF was in force at the time rule 1.7A commenced. Rule 1.7A generally prescribes modifications of the PSPF as it is incorporated by these rules.

Item 5 – Subrule 1.4(2)

1.24. This item defines the term ***relevant PSPF control*** by reference to rule 4.3.

1.25. The term 'relevant PSPF control' is used throughout these rules to refer to the individual requirements in the PSPF that have been incorporated by these rules (refer rule 4.3).

1.26. The use of the term 'control' rather than the term 'requirement' is deliberate and reflects the terminology adopted in the Accreditation Rules. Although the PSPF refers to requirements, the Accreditation Rules uses the term 'controls' to describe the specific controls entities must meet and comply with. The use of control does not alter the meaning of the PSPF requirements themselves but ensures that those PSPF requirements are to be interpreted and applied within the context of the Accreditation Rules.

Item 6 – Subrule 1.7(2)

1.27. This item repeals and substitutes subrule 1.7(2) with a new subrule which sets out the application of amendments to incorporated instruments.

1.28. New subrule 1.7(2) provides for the time period for compliance with any changes to incorporated instruments. For changes made to the PSPF after these Amendment Rules commence, accredited entities will have a 3 month period after the change takes effect. For other incorporated instruments, a 12 month period applies.

1.29. The effect of paragraph 1.7(2)(a) is that, unless the contrary intention appears, an entity is not required to comply with changes to the PSPF until 3 months after that change takes effect. It is limited to changes to the PSPF that occur after the commencement of these rules. Therefore, the PSPF issued on 24 July 2025 by the Department of Home Affairs will apply immediately from the commencement date of these Amendment Rules.

1.30. A change to the PSPF is taken to take effect on the date it is published on the PSPF website by the Department of Home Affairs unless specified otherwise. Following the date of publication, entities have a 3 month period to comply with any changes.

1.31. Previously, these Rules did not incorporate external frameworks like the PSPF by reference. Instead, compliance with the PSPF was through complying with the controls

listed in Schedule 5 of the Rules. As a result, any updates to the PSPF rules would not automatically apply until the Rules themselves were amended.

1.32. These rules take a new approach to how the relevant PSPF controls apply. The relevant PSPF controls are now incorporated by reference. This means that future updates to the relevant PSPF controls will be, by operation of law, incorporated by these Rules. This will provide greater alignment between the PSPF and the Rules.

1.33. To support this new approach, a 3 month period has been introduced which provides entities with a reasonable period to comply with changes to the PSPF. This period is considered appropriate to provide entities time to take the necessary actions to comply with the PSPF controls in rule 4.3, such as updating relevant documentation or otherwise. This time period also takes into account that changes to those controls from one annual release of the PSPF to the next are expected to be minor in nature.

1.34. Paragraph 1.7(2)(b) prescribes that accredited entities are not required to comply with changes to other incorporated instruments until 12 months after that change takes effect.

1.35. There is no change to the period when a change to any other incorporated instruments applies. Consistent with current arrangements, entities will not be required to comply with a change to any other incorporated instruments until 12 months after that change takes effect. This rule recognises that an accredited entity may not be able to immediately comply with a change to an incorporated instrument and ensures that entities are provided sufficient time to implement, where required, IT system upgrades or other arrangements to comply with the requirements.

1.36. This approach takes into account the need for timely implementation of changes to protective security frameworks and the practical realities faced by entities in achieving compliance with these obligations in a fast-evolving environment.

Item 7 – After rule 1.7

1.37. This item inserts new rules 1.7A and 1.7B, which provide for the modification of the PSPF and ISO/IEC 27001 for the purposes of incorporation or application of the PSPF or the standard by these Rules, respectively.

1.7A Modifications of the PSPF

1.38. Paragraph 1.7A(a) provides that references in the PSPF to ‘Australian Government Resources’ or ‘Australian Government people and resources’ are taken to be references to ‘DI data environment’ in the Rules.

1.39. Paragraph 1.7A(b) provides that references to ‘risk’ in the PSPF are taken to mean ‘cyber security risk’ within the meaning of the Rules.

1.40. The effect of this provision is to deem certain terms in the PSPF to mean another term within the meaning of the Accreditation Rules. The purpose of these modifications is to tailor the PSPF within the Rules to prevent ambiguity and support effective operation of PSPF obligations in a DI data environment.

1.7B Modifications of ISO/IEC 27001

1.41. The effect of this provision is to deem certain terms in a specified ISO/IEC 27001 standard to mean another term within the meaning of the Digital ID Act. The purpose of these modifications is to tailor ISO/IEC27001 within the scope of the Rules.

1.42. The purpose is also to prevent ambiguity and support effective operation of ISO/IEC27001 in a DI data environment.

Item 8 – Subparagraph 3.3(1)(a)(i)

1.43. This item repeals and substitutes subparagraph 3.3(1)(a)(i).

1.44. This amendment uses the new defined term ***protective security framework controls.***

1.45. Previously, this provision referred to implementation of, and compliance with, the controls in the protective security framework it uses, or will use if accredited.

1.46. New subparagraph 3.3(1)(a)(i) is substantially the same in effect to previous subparagraph 3.3(1)(a)(i) which also relates to the protective security assessment by an accredited entity or an accreditation applicant.

1.47. The only substantive change to this provision is to specifically refer to rule 4.2, which provides for the protective security framework controls which an entity must comply with, or will comply with if accredited. The provision is also amended to include more precise language by using the new defined term 'protective security framework controls' and to clarify that that entities must comply with, or will comply with if accredited, those controls for the purposes of rule 4.2.

1.48. The purpose of this amendment is to ensure the protective security assessment is conducted in alignment with the relevant controls listed under subrule 4.3(1) instead of assessing an entire framework.

Item 9 – Subparagraph 3.3(1)(a)(iii)

1.49. This item omits 'Division 2' and substitutes 'Division 3' in subparagraph 3.31(1)(a)(iii).

1.50. The purpose and effect of this item is to correct a typographical error in the provision reference.

1.51. Subparagraph 3.3(1)(a)(iii) is intended to require the protective security assessment of an accredited entity to include the additional protective security controls in new Division 3 of Part 4.1 of Chapter 4.

1.52. For completeness, the protective security controls in Division 3 of Part 4.1 of Chapter 4 are required to be reviewed and assessed as part of the protective security assessment by existing subparagraph 3.3(1)(a)(i).

Item 10 – Subrule 3.5(1)

1.53. This item omits "a particular protective security control in the framework it implements" and substitute "a particular protective security framework control".

1.54. This change reflects the insertion of the new definition of ***protective security framework control*** and the associated implications around complying with a control.

Items 11, 12 and 13 – Subrule 3.5(1), subparagraph 3.5(1)(c)(i), subrule 3.5(2)

1.55. These items amend subrule 3.5(1), subparagraph 3.5(1)(c)(i) and subrule 3.5(2), substituting references to "implement" with "comply with'. This creates consistency with the revised language around controls with the rules.

1.56. This change reflects the terminology introduced in the new definition of *protective security framework control.* The effect is to clarify that entities must comply with controls, not solely implement frameworks.

Item 14 – Division 2 of Part 4.1 of Chapter 4 (heading)

1.57. This item repeals and substitutes the heading to "Division 2 – Protective security framework controls".

1.58. The effect of this heading change is to reflect the revised terminology and structure of the chapter.

Item 15 – Rules 4.2 to 4.4

1.59. This item repeals and substitutes rules 4.2 to 4.4.

4.2 Accredited entities must comply with protective security framework controls

1.60. Rule 4.2 provides for the protective security framework controls which apply to an accredited entity.

1.61. Accredited entities that are NCEs must comply, in respect of their accredited services and DI data environment, with the relevant PSPF controls in accordance with the PSPF. This is consistent with broader Australian government policy that NCEs must comply with the PSPF.

1.62. Accredited entities that are not an NCEs must comply with either all of the controls specified in ISO/IEC 27001 or the controls of an alternative framework in accordance with rule 4.5. This change means that an accredited entity that is not an NCE will not be able to select the PSPF as their protective security framework.

1.63. This change has been made to reflect the intended scope of the PSPF, which is designed primarily for Australian Government entities. The PSPF provides direction and guidance for Accountable Authorities of NCEs and contains detailed requirements for the protection, handling, and disposal of Australian Government information and resources. These requirements are tailored to the classification and handling of Australian Government information and do not extend to non-government information, making the PSPF unsuitable for other types of entities.

1.64. Restricting the use of the PSPF to NCEs ensures appropriate application of the PSPF within the accreditation framework and avoids misapplication by entities for whom the PSPF was not designed.

1.65. NCEs are subject to a ministerial directive issued by the Minister for Home Affairs which mandates the application of the PSPF to the extent required by legislation. This directive operates alongside the PGPA Act, establishes the PSPF as Australian Government policy and promotes a whole-of-government approach to protective security to support the secure and effective delivery of government business.

1.66. The phrase "in accordance with" in rule 4.2 ensures controls are applied within the context of the relevant protective security framework. This means that entities must apply the controls in a way that reflects how they are intended to operate within the structure of the applicable framework.

1.67. For example, a key component of requirement 0018 of the PSPF is compliance with mandatory elements in table 1 of the PSPF. Although table 1 of the PSPF has not been incorporated, entities must implement requirement 0018 in accordance with the context of the PSPF, including Table 1.

1.68. Similar to current subrule 4.3(2), new subrule 4.2(3) prescribes that subrule 4.2 is subject to rule 4.6.

4.3 Relevant PSPF Controls

1.69. New rule 4.3 sets out the relevant PSPF controls that an NCE must comply with in respect of its accredited services and DI data environment, for the purposes of rule 4.2. The relevant PSPF controls must be complied with in accordance with the PSPF.

1.70. The rationale for this change is to align protective security controls with the specific risks and operational contexts of the digital ID system, focusing on the relevant controls that are most relevant to the digital ID system.

1.71. The effect of this change is that accredited entities must remain aligned with the most current version of the incorporated frameworks. This improves consistency with whole-of-government policy and ensures that protective security obligations reflect contemporary standards.

1.72. The table at rule 4.3 prescribes the PSPF controls that an entity must comply with. Column 1 sets out the PSPF control number. Column 2 prescribes the relevant PSPF requirement that an entity must meet to implement each PSPF control for the purposes of rule 4.2.

1.73. As a result of the operation of subrule 1.7(2), an accredited entity is not required to comply with a change to the PSPF controls as incorporated by subrule 4.3(1) until 3 months after the change to the PSPF has taken effect.

1.74. This item repeals 4.3(4) as Schedule 5 has become obsolete and the relevant requirements of the PSPF are now listed in the table at subrule 4.3(1).

Item 16 – Subrules 4.5(1) to (3)

1.75. Item 16 repeals and substitutes subrules 4.5(1) to (3).

1.76. Previously, under subrule 4.5(1), any accredited entity may implement an alternative protective security framework if they meet certain requirements, which generally is to

demonstrate compliance with all of the same kinds of controls that would be required if the entity were to implement either PSPF or ISO/IEC 27001 for the purposes of previous rule 4.2.

1.77. New subrule 4.5(1) provides that an accredited entity (other than an NCE) may only comply with the controls of an alternative framework if they demonstrate, in accordance with subrule 4.5(2), that the entity complies with all the same kinds of controls specified in ISO/IEC 27001.

1.78. The effect of this amendment is to:

- limit the types of entities that may comply with an alternative framework to any entity that is not an NCE; and
- require relevant entities to demonstrate compliance with all the same kinds of controls specified in ISO/IEC 27001, and not the PSPF.

1.79. The purpose of this amendment is to give effect to the overarching policy intention of allowing only NCEs to comply with PSPF.

1.80. Previously, subrule 4.5(2) provided for an entity's compliance with the PSPF. This provision is repealed and not replicated as it does not reflect the policy intention.

1.81. New subrule 4.5(2) replicates the effects of previous subrule 4.5(3), which provides for an entity's compliance with all the same kinds of controls as ISO/IEC 27001. Under new subrule 4.5(2), an accredited entity that complies with an alternative framework must prepare and maintain an up-to-date document that maps each control in the alternative framework that must be complied with against controls in ISO/IEC 27001. The document must specify any ISO/IEC 27001 controls that are not covered because the alternative framework does not require compliance with those controls.

1.82. This ensures that, for entities seeking to comply with an alternative framework, the framework is equivalent in substance to ISO/IEC 27001 and supports continues to support the policy intention that the entity meets appropriate security requirements.

Item 17 – Subrule 4.5(4)

1.83. This item omits "If an accredited entity implements an alternative framework for the purposes of rule 4.2" and substitutes it with "If an accredited entity complies with the controls of an alternative framework for the purposes of paragraph 4.2(1)(b)".

1.84. This amendment removes references to 'implement' and substitutes it with 'complies with' in order to clarify that entities must comply with specific controls and not merely implement frameworks.

1.85. As discussed above, the purpose of this terminology update is to reinforce a compliance-based approach to the rules.

1.86. While the effect of Item 16 is to remove existing subrule 4.5(3), the numbering of this provision remains subrule 4.5(4) to reflect common drafting practice not to renumber in these instances.

Item 18 – Paragraph 4.5(4)(a)

1.87. This item omits ", and manage and monitor" to ensure coherency with terminology within this Division.

1.88. The phrase 'manage and monitor' is considered obsolete, as those obligations are implicit in the requirement to comply with controls effectively under the compliance-based approach.

Item 19 – Subparagraph 4.5(4)(a)(ii)

1.89. This item omits "or (3)(b)" and substitutes it with "of this rule".

1.90. This is a consequential amendment to reflect the repeal of subrule 4.5(3) in Item 16.

Item 20 – Subrule 4.5(6)

1.91. This item repeals subrule 4.5(6).

Item 21 – Rule 4.6

1.92. This item omits "a particular control in the framework it implements" and substitutes it with "a particular protective security framework control", to reflect the new term protective security framework control.

Item 22 – Rule 4.9 (note)

1.93. This item repeals the Note under rule 4.9.

1.94. This is to remove any confusion from referencing obsolete policies that are no longer in circulation or no longer exist.

Item 23 – Subrule 4.12(2)

1.95. This item repeals and substitutes subrule 4.12(2).

1.96. Rule 4.12 sets out the requirements for system security plans. Currently, subrule 4.12(2) provides for the system security plan requirements if an accredited entity implements the PSPF. Relevantly, the entity's system security plan is to be the security plan referred to in PSPF Policy 11 (Robust IT systems).

1.97. PSPF Policy 11 is from an outdated PSPF Release and is not the current PSPF policy, as published by the Department of Home Affairs.

1.98. New subrule 4.12(2) provides that if an accredited entity complies with the relevant PSPF controls for the purposes of rule 4.2, the entity's system security plan is the plan referred to in section 3.1 of the PSPF, which deals with security planning. It also provides that the plan must contain any other information required by these Amended Rules to be included in the entity's system security plan.

1.99. New rule 4.2 confines the compliance of PSPF to only NCEs. The effect of this provision is that the NCEs system security plan must comply with section 3.1 in the PSPF, which is incorporated by reference from time to time.

Item 24 – Subrule 4.13(2)

1.100. This item omits "If an accredited entity implements ISO/IEC 27001" and substitutes it with "If an accredited entity complies with ISO/IEC 27001 for the purposes of rule 4.2", to reflect the revised terminology of "complying with" ISO/IEC 27001.

1.101. This is consistent with the language used throughout the amended rules.

Item 25 – After Chapter 7

1.102. This item inserts new Chapter 8, which contains the application, saving and transitional provisions.

8.1 Transitional provision for amendments made by Schedule 1 to the *Digital ID (Accreditation) Amendment (PSPF and Other Measures) Rules 2025*

1.103. Subrule 8.1(1) provides that this rule applies to an application for accreditation made, but not finally determined, before the commencement day. Subrule 8.1(2) relevantly provides that despite the amendments made by Schedule 1, the old rules continue to apply on or after the commencement day in relation to that application, as if those amendments had not been made.

1.104. Subrule 8.1(3) provides for defined terms used in this rule, which are ***amending instrument***, ***commencement day*** and ***old rules***.

1.105. The effect of 8.1 is that any application for accreditation which is not decided before the day that rule 8.1 commences will continue to be assessed under the Accreditation Rules that were in force immediately before the commencement date. This rule saves any on-hand applications which are not decided immediately before the commencement date and ensures that the rules which applied to the entity at the time of application will continue to apply to that application.

1.106. This ensures procedural fairness and avoids the retrospective application of new requirements.

Item 26 – Schedule 5

1.107. This item repeals Schedule 5 as the relevant PSPF controls have now been incorporated by reference within these amendments.

Schedule 2—Duration of consent

Item 1 – Paragraph 4.41(3)(d)

1.108. This item repeals and substitutes paragraph 4.41(3)(d) in the Accreditation Rules.

1.109. Section 45 of the Digital ID Act broadly prohibits an accredited entity from disclosing certain attributes of an individual to a relying party when verifying that individual's identity, digital ID, or information about them. However, the accredited entity may disclose that information to a relying party if they obtained the individual's express consent. The information could include the individual's current name or former name, address, date of birth, phone number or email address. The Digital ID Act does not specify an expiry period for an individual's express consent.

1.110. Rule 4.41 sets out the duration of express consent given by an individual. Broadly, it provides for the requirements around any express consent given by an individual for the future collection, use or disclosure of their personal information.

1.111. This provision also provides strong safeguards around that consent. Subrule 4.41(2) relevantly requires an accredited entity to provide the individual with a clear and simple process to vary or withdraw any consent. In addition, subrule 4.41(4) relevantly prohibits an accredited entity from relying on consent given in accordance with subrule 4.41(1) if that consent has been withdrawn or expired.

1.112. Subrule 4.41(3) broadly sets out the period when the consent expires. The effect of that provision is that consent expires at the earliest of the periods described in that provision. Paragraph 4.41(3)(d) broadly provides for consent to expire 12 months after the consent was initially given.

1.113. The effect of Item 1 is to provide for two different periods of consent which applies depending on the circumstances.

1.114. New subparagraph 4.41(3)(d)(i) relevantly provides that if the accredited entity is an Attribute Service Provider (ASP) and the individual declares in their consent that their use of the entity's accredited services is for or on behalf of a business (including a business carried on by that individual) – the consent expires 7 years after the consent was initially given.

1.115. New subparagraph 4.41(3)(d)(ii) broadly provides for a 12 month consent period in any other circumstances.

1.116. An ASP is an entity that provides, or proposes to provide, a service that verifies and manages an attribute of an individual, as defined in section 9 of the Digital ID Act. In some circumstances an individual may choose to use a Digital ID provided by an Identity Service Provider (ISP), in combination with an additional attribute/s provided by an ASP, in order to access an online service provided by a relying party.

1.117. For example, a person responsible for a business wants to access government online services to lodge business activity statements on behalf of the business. They use their personal Digital ID issued by an ISP to verify their digital identity. To demonstrate their authority to act on behalf of the business, the person uses an ASP accredited service

that verifies and manages the attribute/s, confirming their business relationship. The government agency (the relying party) accepts both the personal Digital ID and the business authority attribute/s to grant the person access to the service.

1.118. Without the proposed amendment, consent for the use of attributes managed by an ASP is limited to a 12 month period in all circumstances. This amendment allows for two different consent periods: a 7 year period where consent is given to an ASP for on behalf of a business (as illustrated in the example above), and a 12 month period in all other cases.

1.119. The current 12 month expiry period for express consent for individuals reflects a privacy-protective approach consistent with the Office of the Australian Information Commissioner's Australian Privacy Principles Guidelines, which provide that express consent should not be enduring. The shorter period is appropriate in the context of personal use, which requires regular renewal to ensure that consent remains valid and informed.

1.120. By contrast, businesses often operate under contractual and internal governance frameworks that support long term or ongoing relationships with individuals acting on their behalf. The 7 year consent duration is intended to apply to a range of relationships that a person may have with a business. Scenarios may include individuals who are employees, contractors, unpaid volunteers, or sole traders operating their own business. It also includes individuals who are authorised to act as agents for a business, such as tax agents or other professional representatives. These individuals often have relationships with multiple businesses.

1.121. Requiring authorised representatives and agents to renew their express consent every 12 months creates an unnecessary administrative and regulatory burden and may impact business productivity and services. The 7 year expiry period for express consent given to ASPs for or on behalf of a business takes into account these differences, while ensuring that the express consent given is not enduring and can be withdrawn at any time.

1.122. Item 1 does not change any other existing requirements under rule 4.41, including the requirements on accredited entities with public-facing accredited services to have clear and simple processes in place for an individual to vary or withdraw their consent. In particular, the proposed amendment does not affect other consent periods set out under subrule 4.41(3), which means that a consent given under subrule 4.41(1) can have a different expiry period to 12 months or 7 years.

1.123. This amendment introduces flexibility to support efficient and sustainable business use of accredited services while continuing to reinforce the broader intent of rule 4.41, which is to ensure that express consent is meaningful, time-bound, and tailored to the context in which it is given.

Schedule 3—Suspension and resumption

Item 1 – Subrule 1.8(1)

1.124. Item 1 omits "starting on the day that is 12 months after the day on which these rules commence" and substitutes "on and after 30 November 2025" in subrule 1.8(1) of the Accreditation Rules.

1.125. Rule 1.8 broadly provides for the application of certain provisions to a transitioned accredited entity.

1.126. A transitioned accredited entity is defined in rule 1.4 as an entity taken to be accredited immediately after commencement of the Act, in accordance with item 2 of Schedule 1 to the *Digital ID (Transitional and Consequential Provisions) Act 2024*.

1.127. Subrule 1.8(1) generally provides that the provisions listed in a table under subrule 1.8(1) apply to transitioned accredited entities starting on the day that is 12 months after the day on which the Accreditation Rules commence. The Accreditation Rules commenced on 30 November 2024.

1.128. The effect of Item 1 is to provide for the provisions in that table to apply on and after 30 November 2025. Specifying a date provides more clarity and certainty to accreditation applicants and accredited entities on the application of these provisions.

Item 2 – Subrule 1.8(1) (table items 11 and 12)

1.129. Item 2 repeals table items 11 and 12 in the table under subrule 1.8(1).

1.130. Items 11 and 12 of the table provides for the application of rule 5.7 and subrule 5.9(2) to transitioned accredited entities.

1.131. These provisions are now relocated in new subrule 1.8(1A), inserted by Item 3.

1.132. This amendment is a consequential amendment to Item 3.

Item 3 – After subrule 1.8(1)

1.133. Item 3 inserts new subrule 1.8(1A) after subrule 1.8(1).

1.134. This Item provides that rule 5.7 and subrule 5.9(2) apply to a transitioned accredited entity on and after 30 November 2026.

1.135. Rule 5.7 broadly requires ISPs to implement an individual's request to temporarily suspend the use of their digital ID as soon as practicable after confirming the legitimacy, and notify the individual of the suspension and how to resume the use of the digital ID.

1.136. Rule 5.8 separately provides for suspension in cases of suspected fraud or cyber security incidents.

1.137. Rule 5.9 generally provides for resuming the use of a digital ID. Broadly, subrule 5.9(2) prescribes the steps an ISP must take to resume use of a digital ID suspended under subrule 5.9(2), including ensuring the individual completes identity proofing at the same identity proofing level (IP level) as prior to suspension.

1.138. IP levels, ranging from IP1 to IP4, reflect the strength and confidence of identity verification required for different services. The higher the IP level, the more robust and reliable the identity verification process becomes, with higher levels necessitating more comprehensive checks, such as biometric verification and at the highest IP level an in-person verification.

1.139. The effect of the amendment in Item 3 is that transitioned accredited entities have until 30 November 2026 before the requirements under Rule 5.7 and subrule 5.9(2) apply. As these requirements are about the voluntary suspension and resumption of digital IDs by an ISP, it will only affect accredited ISPs.

1.140. As at the date of this amendment, the transitioned accredited entities that are ISPs, as prescribed in Table 1 of Schedule 1 to the *Digital ID (Transitional and Consequential Provisions) Rules 2024*, include the Commissioner of Taxation, Australian Postal Corporation, Makesure Pty Ltd, and OCR Labs Pty Ltd.

1.141. Accordingly, as at the date of this amendment, it applies to the Commissioner of Taxation, Australian Postal Corporation and Makesure Pty Ltd in relation to the obligations under Rule 5.7 and subrule 5.9(2) of the Digital ID Rules. It does not apply to apply to OCR Labs Pty Ltd which supports only one-off identity verification and does not involve the issuance of reusable digital IDs to which these obligations would apply.

1.142. The purpose of this amendment is to provide the relevant transitioned accredited entity with an additional 12 months to comply with these requirements. This is in response to feedback from select transitioned accredited entities that these requirements have proven operationally and technically challenging to implement into their existing digital ID services. This includes the prospect, in some circumstances, of inadvertently preventing individuals from resuming the use of their suspended digital ID where the individual cannot re-verify their identity to the original IP level.

1.143. The deferred application of these provisions allows transitioned accredited entities additional time to comply with the law, including implementing technically demanding requirements, particularly around identity proofing requirements relating to digital ID suspension and resumption operation.

1.144. Subrule 5.9(1) applies only where resumption is required due to a suspension under rule 5.7. If a digital ID is not suspended under rule 5.7, subrule 5.9(1) will not apply by default.

Item 4 – Subrule 1.8(2)

1.145. Item 4 omits “subrule 1” and substitutes “subrule (1)” to “subrules (1) or (1A)”.

1.146. This is a consequential amendment to the amendments in Items 2 and 3.