EXPLANATORY STATEMENT

Issued by authority of the Minister for Finance

Digital ID Act 2024

Digital ID Amendment (Redress Framework 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 Rules 2024* (Digital ID Rules) establish a robust legal framework governing applications and obligations to participate in the Australian Government Digital ID System (AGDIS).

The *Digital ID Amendment (Redress Framework and Other Measures) Rules 2025* (Amendment Rules) amends the Digital ID Rules to strengthen support for digital ID users within the Australian Government Digital ID System (AGDIS) and improve the efficient operation and regulation of the AGDIS. In particular, the Amendment Rules:

- establish a redress framework under section 88 of the Digital ID Act for cyber security and digital ID fraud incidents relating to accredited services within the AGDIS.
- establish a streamlined application for approval to participate in the AGDIS, for Commonwealth, State or Territory government participating relying parties that are affected by machinery of government (MOG) changes.
- authorise the Digital ID Data Standards Chair to use the digital ID accreditation trustmark.
- improve the System Administrator's oversight of cyber security incidents and digital ID fraud incidents.

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 commence 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
Data Standards Chair	Digital ID Data Standards Chair
Digital ID Regulator	The Digital ID Regulator is the Australian Competition and Consumer Commission as defined in section 90 of the Digital ID Act
Digital ID trustmark	Digital ID Accreditation Trustmark
ISP	Identity Service Provider
IXP	Identity Exchange Provider
MOG	Machinery of government

ATTACHMENT A

Details of the *Digital ID Amendment (Redress Framework and Other Measures) Rules 2025*

Section 1 – Name

1.1. This section provides that the name of this instrument is the *Digital ID Amendment (Redress Framework 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—Redress framework

Overview

1.7. Subsection 88(1) of the Digital ID Act relevantly provides that the *Digital ID Rules 2024* (Digital ID Rules) must provide for or in relation to a redress framework for incidents that occur in relation to accredited services of accredited entities that are provided within the Australian Digital ID System (AGDIS). The redress framework must be provided for within 12 months of commencement of the Digital ID Act, which was 30 November 2024.

1.8. Subsection 88(2) of the Digital ID Act sets out a list of matters that the Digital ID Rules made for the purposes of subsection 88(1) must deal with.

1.9. Schedule 1 to the Amendment Rules provides for a redress framework for cyber security incidents and digital ID fraud incidents that occur in relation to accredited services of accredited entities within the AGDIS.

1.10. The AGDIS is the digital ID system overseen and maintained by the Digital ID Regulator in accordance with section 58 of the Digital ID Act. The Digital ID Act deals with the accreditation of digital ID services that may operate within digital ID systems including but not limited to the AGDIS. The Digital ID Regulator is supported by a System Administrator who, in accordance with section 95 of the Digital ID Act, is responsible for operational risks, including digital ID fraud and cyber security incidents in relation to the AGDIS.

1.11. Consistent with the revised Explanatory Statement to the Digital ID Act, the purpose of this redress framework is to support consumers' ability to efficiently deal with and get assistance in relation to digital ID fraud incidents and cyber security incidents occurring in relation to accredited services provided within the AGDIS.

1.12. Providing individuals with access to appropriate redress is an important element in ensuring the integrity of the AGDIS. It encourages participating accredited entities to be accountable for incidents that occur in relation to their services, to strive for continued improvement, and promotes public confidence in the safeguards and outcomes of using digital ID.

1.13. To support the successful uptake of digital ID by entities and individuals, the redress framework must balance the regulatory burden on entities, which may disincentivise participation in the AGDIS, with the need to provide meaningful redress to affected individuals within the AGDIS, thereby fostering public confidence in the system.

1.14. The Amendment Rules seek to balance these policy considerations by establishing a redress framework that places the following requirements on certain entities within the AGDIS:

- to make reasonable attempts to notify individuals affected by a digital ID fraud incident or cybersecurity incident, where appropriate;
- to refer unresolved technical issues to the System Administrator, in certain circumstances who may then recommend a course of action to the entity;

- to provide information, support and assistance to individuals affected by incidents in certain circumstances;
- to develop and publish policies relating to complaints;
- to develop and publish policies relating to the identification, management and resolution of cybersecurity incidents and digital ID fraud incidents.

1.15. These requirements include matters which must be dealt with by the Digital ID Rules made for the purposes of subsection 88(1) of the Digital ID Act.

1.16. The redress framework complements broader Commonwealth legislation, such as the *Privacy Act 1988* (Privacy Act). It also complements pre-existing provisions in the Digital ID Rules and the *Digital ID (Accreditation) Rules 2024* (Accreditation Rules) that deal with providing support and assistance to individuals in relation to cyber security incidents and digital ID fraud incidents. In this way, the digital ID legislative framework will ensure that appropriate safeguards and redress mechanisms are in place for users of digital ID services within the AGDIS.

Item 1 – After Chapter 4

1.17. This amendment inserts 'Chapter 4A – Redress Framework' after Chapter 4 of the Digital ID Rules.

1.18. New Chapter 4A provides for a redress framework in the Digital ID Rules. It contains 5 Parts, with each part dealing with one or more of the matters which the Digital ID Rules must deal with under subsection 88(2) of the Digital ID Act:

- *Part 1 – Preliminary* deals with entities that are covered by the framework, which relates to paragraph 88(2)(a) of the Digital ID Act.
- *Part 2 – Notifying affected individuals of incidents* deals with the matters required by paragraphs 88(2)(b) and (d) of the Digital ID Act.
- *Part 3 – Referring unresolved technical issues to the System Administrator* deals with the matters required by paragraphs 88(2)(b) and (c) of the Digital ID Act.
- *Part 4 – Providing information, support and assistance to individuals affected by incidents* deals with the matters required by 88(2)(e) of the Digital ID Act.
- *Part 5 – Policies relating to incidents and complaints* deals with the matters required by paragraphs 88(2)(b), (f) and (g) of the Digital ID Act.

1.19. The redress framework provides new requirements on Attribute Service Providers (ASP) and Identity Service Providers (ISP) participating in the AGDIS, or whose approval to participate has been suspended or revoked. The scope of this framework strikes a careful balance between the risk of harm to individuals and the AGDIS, as well as the regulatory burden on participating entities.

Part 1 – Preliminary

4A.1 Application of this Chapter

1.20. Subrule 4A.1(1) relevantly provides that, for the purposes of subsection 88(1) of the Digital ID Act, this Chapter provides for a redress framework for incidents that occur in relation to accredited services within the AGDIS.

1.21. Subrule 4A.1(2) sets out the entities to which this Chapter applies. Relevantly, it provides that this Chapter applies to an ASP or an ISP that is a participating entity, or an entity whose approval to participate is suspended or revoked. This provision specifically deals with the matters under paragraph 88(2)(a) of the Digital ID Act, which provides for the entities covered by the framework.

1.22. Rule 1.4 of the Digital ID Rules sets out the definitions in these rules. Relevantly, subrule 1.4(1) provides that unless otherwise specified, expressions defined in the Accreditation Rules have the same meaning in these rules. Accordingly, the terms 'ASP' and 'ISP' take the meaning as defined in the Accreditation Rules as they are not specified in the Digital ID Rules. The term 'participating entity' is defined in rule 1.4 of the Digital ID Rules, which means an entity that holds an approval to participate in the AGDIS.

1.23. The redress framework has been limited to apply to ASPs and ISPs. This recognises that these types of accredited service providers within the AGDIS will be expected to assist users with digital ID related incidents covered by the Digital ID Act. The regulatory scope of AGDIS is around the provision and use of accredited services in that system. This is consistent with the intent of a redress framework in relation to incidents that occur in relation to accredited services under section 88 of the Digital ID Act. For that reason, Identity Exchange Providers (IXP) are not included because they do not directly provide services to individual users in the AGDIS.

1.24. Note 1 under subrule 4A.1(2) is intended to inform readers that there are other provisions in the Digital ID Rules and the Accreditation Rules that relate to cyber security incidents and digital ID fraud incidents, although those provisions apply in other broader circumstances (i.e. those provisions are not limited to the provision of accredited services within the AGDIS) or where the incident affects an individual.

1.25. Accordingly, this Chapter focusses on providing a redress framework for cyber security and digital ID fraud incidents in relation to accredited services within the AGDIS. The redress framework focusses on cyber security and digital ID fraud incidents as these are the kinds of incidents which may result in an adverse outcome or harm for individuals.

1.26. Note 2 under subrule 4A.1 informs readers that Part 5 of this Chapter has a narrower application than that which is provided for by subrule 4A.1(2) (see rule 4A.6). These Notes are inserted to assist the reader.

Part 2 – Notifying affected individuals of incidents

4A.2 Notifying affected individuals of incidents

1.27. This rule provides for the notification of individuals following a cyber security incident or digital ID fraud incident. It specifically engages with the matters in paragraph 88(2)(d)

of the of the Digital ID Act, which provides for the redress framework to deal with requirements relating to notifying individuals that are covered by the framework.

1.28. Subrule 4A.2(1) relevantly provides that this rule applies to cyber security incidents or digital ID fraud incidents that occur, or are reasonably suspected of having occurred, in relation to an accredited service provided by an entity within the AGDIS. This rule applies to entities as set out in subrule 4A.1(2).

Considering whether it is appropriate to notify an individual

1.29. Paragraph 4A.2(1)(a) relevantly provides that an entity must consider whether it is appropriate to notify each individual affected by a cyber security incident or digital ID fraud incident.

1.30. Subrule 4A.2(2) sets out the factors which an entity must take into account when considering whether it is appropriate to notify an individual. These factors seek to balance the potential harm to the individual resulting from the incident itself, as well as the risk that, in some circumstances, notification may exacerbate harm to the individual and the AGDIS. In practice, this could include consideration of whether the entity has trusted contact details for the individual. In some circumstances, it may not be appropriate to notify the individual if this could also alert the malicious actor.

1.31. The purpose of this provision is to ensure that the individual is not inadvertently harmed or left worse-off if they are notified of an incident.

1.32. The term 'material effect' is defined in rule 1.4 of the Digital ID Rules. In this context, a material effect on the AGDIS could be triggered if the notification of the individual could exacerbate the incident to a magnitude that would cause the degradation or loss of functionality within the AGDIS, or limit the ability of an entity to participate in the AGDIS. For example, this could occur if the notification alerted the malicious actor and resulted in a cyber security incident or digital ID fraud incident with greater impact.

Making reasonable attempts to notify an individual

1.33. Paragraph 4A.2(1)(b) provides that if the entity is satisfied that it is appropriate to notify the individual, they must make reasonable attempts to do so. The purpose of this provision is to recognise that, when it is appropriate to do so, it is in the best interests of the individual to be aware of the incident. This would enable them to mitigate any flow-on consequences that could impact other transactions or services where they have used their digital ID, and for transparency.

1.34. This provision requires entities to make a reasonable attempt to notify the individual, which should be done in consideration of the time and method of the attempt and the likelihood that the attempt would be successful. This provision recognises that an entity's reasonable attempt to notify an individual may not be successful. This could be due to myriad reasons, including that the individual is not available or the entity does not have the current contact details of the individual.

1.35. This rule applies in addition to any obligations an entity may have under Part IIIC of the Privacy Act (relating to the notification of eligible data breaches).

1.36. The requirement to notify an affected individual under rule 4A.2 does not prescribe a specific timeframe within which to do so. This provides for circumstances where it may not be appropriate to notify the individual immediately.

1.37. This rule also operates alongside paragraph 4.2(3)(g) of the Digital ID Rules, which is about notifying the System Administrator whether the individual was affected by the incident. Whilst the notification to the System Administrator under rule 4.2 must be made within the timeframes specified in subrule 4.2(4), this does not preclude the entity from notifying the individual under rule 4A.2 outside of these timeframes.

Part 3 – Referring unresolved technical issues to the System Administrator

4A.3 Unresolved technical issues must be referred to the System Administrator

1.38. This rule provides for the referral of unresolved technical issues to the System Administrator where the issues result from a cyber security or digital ID fraud incident. It specifically deals with the matters under paragraph 88(2)(c) of the Digital ID Act which provides for procedures for dealing with incidents.

1.39. The purpose of this rule is to promote trust in the AGDIS by providing individuals with greater confidence that appropriate redress will be provided. It is also intended to promote accountability of entities through referral to the System Administrator.

1.40. Subrule 4A.3(1) sets out the circumstances in which this rule applies.

1.41. Paragraph 4A.3(1)(a) relevantly provides that this rule applies if an incident occurs or is reasonably suspected of having occurred in relation to an accredited service within the AGDIS. This rule applies to entities as set out in subrule 4A.1(2).

1.42. Paragraph 4A.3(1)(b) relevantly provides that this rule applies if, as a result of the incident, an individual is unable to use their digital ID due to a technical issue with the entity's service that is within the control of the entity or another entity to which this Chapter applies.

1.43. The term 'technical issue' is not defined by these rules. It is intended to capture issues of a technical nature that result in an individual being unable to use their digital ID. This could include persistent technical issues that require manual override for remediation. This provision does not allow for an individual to refer their complaints or disputes directly to the System Administrator.

1.44. The technical issue must be within the control of the entity, or another entity to which this Chapter applies. This is intended to capture technical issues that may require a coordinated response from entities across the AGDIS with support from the System Administrator. It is also intended to exclude technical issues which are within the control of the user from being escalated to the System Administrator. For example, forgotten passwords or non-digital ID technology challenges.

1.45. Subrule 4A.3(2) provides the timeframe within which an entity must refer the technical issue to the System Administrator. Broadly, this requires an entity to refer the technical issue as soon as reasonably practicable after the entity becomes aware of the issue which results in an individual being unable to use their digital ID. If the entity became aware of

the technical issue because of a complaint made by the individual, the entity must refer the issue as soon as reasonably practicable and within 28 days after the complaint is made.

1.46. The requirement for the entity to refer the technical issue to the System Administrator within 28 days after the complaint is made provides a service delivery standard to the management of the complaint where it is raised by an individual. This supports the overarching intent of the redress framework to strengthen protection and support for individuals.

1.47. Subrule 4A.3(3) provides the circumstances that must be met before the entity refers the technical issue to the System Administrator under subrule 4A.3(2). The purpose of paragraph 4A.3(3)(a) is to encourage entities to consider whether the issue can be resolved by the entity itself before the referral. Entities should not be referring technical matters which it can resolve itself to the System Administrator. This is also intended to balance the necessity of appropriate referrals with the potential administrative burden on the System Administrator.

1.48. The effect of the term 'reasonably satisfied' is that the entity must be satisfied in the circumstances, to a reasonable level, that the technical issue cannot be resolved without referral to the System Administrator.

1.49. Paragraph 4A.3(3)(b) relevantly provides that the entity must comply with rule 4A.5 (if applicable) before referring to the System Administrator. Rule 4A.5 is about providing an affected individual with information, support and assistance. This is intended to provide support to individuals affected by issues which require referral to the System Administrator. The entity may refer the issue to the System Administrator in circumstances where rule 4A.5 does not apply. For example, in circumstances when the individual is not notified under rule 4A.2, or when the entity becomes aware of the issue other than by complaint made by the individual.

1.50. The Note at subrule 4A.3(3) refers the reader to rule 4A.5.

4A.4 System Administrator may recommend a resolution

1.51. Rule 4A.4 broadly provides that the System Administrator may recommend a resolution to an issue in response to a referral from an entity under rule 4A.3, and some of the potential courses of action that may be recommended.

1.52. New rule 4A.4 only applies in relation to referrals from entities under rule 4A.3. This reflects the role of the System Administrator in providing assistance to entities participating in the AGDIS, and that the System Administrator does not provide dispute resolution.

1.53. The policy intent of this rule is for the System Administrator to provide assistance to entities participating in the AGDIS in relation to dealing with incidents. It is also intended to promote individual users' confidence in the AGDIS by enabling the System Administrator to recommend an independent course of action.

1.54. Subrule 4A.4(2) provides courses of action that the System Administrator may recommend the entity take. This list is not exhaustive; the System Administrator may

recommend another course of action to the entity as appropriate. The courses of action set out in subrule 4A.4(2) are intended to strengthen individual users' confidence in accredited services within the AGDIS by promoting accountability.

1.55. The courses of action set out at subrule 4A.4(2) are limited to reflect the System Administrator's role in supporting entities to manage incidents. They do not include actions which could raise compliance issues, which would be more appropriately addressed by the Digital ID Regulator. This provision does not limit the System Administrator's existing powers under the Digital ID Act.

Part 4 – Providing information, support and assistance to individuals affected by incidents

4A.5 Providing information, support and assistance to individuals affected by incidents

1.56. Rule 4A.5 provides for the provision of information, support and assistance to individuals in certain circumstances. It specifically deals with the matters in paragraph 88(2)(e) of the Digital ID Act, which relates to the provision of information, support and assistance to individuals affected by incidents covered by the framework.

1.57. This rule applies to entities as set out in subrule 4A.1(2).

1.58. This rule sets out when an entity must provide information, support and assistance to an individual affected by a cyber security or digital ID fraud incident where they are notified under rule 4A.2 or when an entity becomes aware of a technical issue mentioned in rule 4A.3 because of a complaint made by an individual. This rule provides for the types of information, support and assistance that must be provided in these circumstances.

1.59. Paragraph 4A.5(2)(a) relevantly provides that an entity must direct the individual to public resources, including information published by the entity on the resolution of incidents and the entity's complaint processes. The effect of this paragraph is that the entity must have available information which would assist the individual in relation to the incident and increase their understanding of the resolution process to the matter. This provision is designed to facilitate entities in empowering individuals to take appropriate actions in the circumstances to mitigate the impact of the cyber security or digital ID fraud incident.

1.60. This paragraph is intended to operate alongside rules 4A.7 and 4A.8, which relate to developing and publishing policies on incident identification and complaint management.

1.61. As set out in Note 1 under subrule 4A.1(2), this rule operates alongside other provisions in the Digital ID Rules and the Accreditation Rules that also deal with providing support and assistance to individuals in relation to cyber security incidents and digital ID fraud incidents.

Part 5 – Policies relating to incidents and complaints

4A.6 Application of this Part

1.62. Rule 4A.6 broadly provides that this Part does not apply to an ASP or an ISP whose approval to participate is suspended or has been revoked.

1.63. This Part relates to the development and publication of certain policies relating to cyber security and digital ID fraud incidents. The effect of this rule is that an entity who is not, at the relevant time, participating in the AGDIS is not subject to these requirements.

1.64. Under section 9 of the Digital ID Act, an entity participates in the AGDIS at a particular time if amongst other things, at that time, the entity holds an approval under section 62 to participate in the AGDIS. Subsection 71(13) of the Digital ID Act relevant provides that if the approval of an entity to participate in the AGDIS is suspended, the entity is taken not to hold the approval while it is suspended.

1.65. The purpose of this provision is to ensure that regulatory burden is appropriately placed on entities who are participating in the AGDIS and ensure they continue to have policies which would be relied upon by digital ID users.

4A.7 Policies relating to the identification etc. of incidents

1.66. This rule relevantly provides that an entity must develop and publish policies relating to the identification, management and resolution of cyber security incidents and digital ID fraud incidents in relation to its accredited services within the AGDIS. It specifically deals with the matters under paragraph 88(2)(f) of the Digital ID Act which provides for the development and publication of policies relating to identification, management and resolution of incidents covered by the framework.

1.67. The effect of this rule is to impose an obligation on entities to have published policies which deals with cyber security incidents and digital ID fraud incidents. The policies could be published on the entity's website or via other means to ensure public access.

1.68. The policies must deal with each of the matters in this rule and in relation to each of the entity's accredited services. For example, if an entity is both an ISP and ASP within the AGDIS, its policies must relate to the identification, management and resolution of cyber security and digital ID fraud incidents for its services as an ISP and an ASP. These policies could be contained in a single document or multiple documents.

1.69. This rule does not require entities to publish policies containing details which may provide threat actors, such as hackers, insights which would negatively affect the AGDIS or digital ID users. The purpose of this rule is to provide assurances to digital ID users that entities providing accredited services within the AGDIS have policies in place around these incidents.

1.70. This rule applies to an ASP or an ISP that is a participating entity, as defined in the Digital ID Rules. As per rule 4A.6, this rule does not apply to an ASP or an ISP whose approval to participate is suspended or has been revoked. This is because an entity whose approval to participate is suspended or revoked does not hold approval to participate in the AGDIS and therefore may not provide or receive services within the AGDIS (section 71 of the Digital ID Act).

4A.8 Policies relating to complaints by individuals

1.71. This rule relevantly provides that an entity must develop and publish policies relating to complaints by individuals relating to cyber security incidents and digital ID fraud incidents. This rule is intended to enhance transparency, empower individuals to navigate

complaint options confidently, and reinforce trust in the Digital ID system. This rule specifically deals with the matters under paragraph 88(2)(g) of the Digital ID Act, which provides for the development and publication of policies relating to complaints by individuals.

1.72. Subrule 4A.8(1) sets out the entities and types of incidents to which this rule applies. This covers a cyber security incident or digital ID fraud incident, or when they are reasonably suspected to have occurred. Similarly to rule 4A.7, this rule applies to an ASP or an ISP that is a participating entity; it does not apply to an ASP or an ISP whose approval to participate is suspended or has been revoked. The policies could be published on the entity's website or via other means to ensure public access.

1.73. Subrule 4A.8(2) provides the minimum content requirements for the complaints policies. The inclusion of these matters in the complaints policies are intended to support individuals to make complaints should they wish to do so, and to provide transparency of the process, procedures and timeframes for dealing with a complaint.

1.74. Subrule 4A.8(3) relevantly provides that this rule may be complied with by way of developing and publishing a policy that relates to complaints generally or in relation to other matters outside of cyber security incidents and digital ID fraud incidents. That is, the entity need not create unique complaints policies for its Digital ID accredited services, so long as the matters in subrules 4A.8(1) and 4A.8(2) are dealt with.

1.75. The effect of this rule is to impose an obligation on entities to have published policies which deal with cyber security incidents and digital ID fraud incidents. The policies could be published on the entity's website or via other means to ensure public access.

1.76. Similar to rule 4A.7, the effect of rule 4A.8 is that published policies must deal with each of the entity's accredited services. For example, if an entity is both an ISP and ASP within the AGDIS, its policies must relate to dealing with individual complaints for its services as an ISP and an ASP. These policies could be contained in a single document or multiple documents.

Schedule 2—Machinery of government changes

Overview

1.77. The AGDIS enables individuals to verify their identity online for certain government services. The AGDIS is overseen and maintained by the Digital ID Regulator under section 58 of the Digital ID Act.

1.78. In general, ***relying parties***, as defined in section 9 of the Digital ID Act, must apply to the Digital ID Regulator for approval to participate in the AGDIS under section 61 of the Digital ID Act. Relying parties may apply for approval to provide, or provide access to, a service as a condition of their approval to participate under subsection 64(3). The Digital ID Regulator can approve the relying party under section 62 of the Digital ID Act and may impose conditions on the approval to participate, including conditions relating to the services a relying party may provide or access under subsection 64(2).

1.79. An approval to participate cannot be transferred or extended to another entity. Broadly, under section 70, the Digital ID Regulator can vary an entity's name in its approval.

1.80. A government ***participating relying party***, as defined in section 9 of the Digital ID Act, can be affected by a Machinery of Government (MOG) change. A MOG change is often, though not always, accompanied by a change to administrative arrangements orders that transfers certain functions, or responsibility for administering certain legislation, from one ministerial portfolio to another. A MOG change can also involve the transfer of functions between entities within the same ministerial portfolio. In either circumstance, if that entity's service/s within AGDIS is expected to transfer to a different entity, the entity receiving the service will need to seek approval to provide that service within the AGDIS. This means that the provision of that service could be disrupted if there are prolonged delays to the application process.

1.81. The Amendment Rules create a streamlined application process which aims to minimise the disruption to services within the AGDIS when a MOG occurs, and to reduce administrative and regulatory burden. It recognises that MOG changes are a routine aspect of government administration and that functions may transfer between entities, at relatively short notice, without substantial alteration to the nature of the services provided, the conditions or the risk environment under which services are delivered. It supports a more efficient approval process while maintaining the integrity of the AGDIS.

1.82. The new streamlined application provisions reduce the mandatory matters that the Digital ID Regulator must consider in approving a relying party to participate in the AGDIS in the relevant circumstances.

Item 1 – subrule 1.4(2)

1.83. Item 1 inserts three new definitional terms into subrule 1.4(2).

1.84. The new terms are: ***receiving entity, transferring entity*** and ***streamlined application***.

1.85. This amendment provides for new terms to be defined by reference to the new definition of ***streamlined applications*** in new rule 1.5.

Item 2 – After rule 1.4

1.86. Item 2 inserts new rule 1.5 'Meaning of ***streamlined application***' after rule 1.4.

1.5 Meaning of streamlined application

1.87. New rule 1.5 provides for the meaning of ***streamlined application***. It relevantly provides that ***streamlined application*** means an application under section 61 of the Digital ID Act made by an entity (the receiving entity) where certain requirements are met.

1.88. First, the ***receiving entity*** is of a kind mentioned in paragraphs (c), (d), (e), (f) and (g) of the definition of *entity* in the Digital ID Act. Broadly, these entities are an Australian Commonwealth, State or Territory or government entity.

1.89. The effect of this requirement is that only entities of the kind in paragraphs (c) to (g) of the definition of entity in the Act can make a streamlined application. While a receiving entity does not have to be of the same kind of entity as a transferring entity, they must be an entity of a kind in paragraphs (c) to (g) of the definition of entity in the Act. The purpose of these requirements is to limit the kinds of entities that can make a streamlined application, as these applications are not intended to be available for all entities.

1.90. Second, the ***transferring entity*** is of a kind mentioned in paragraphs (c), (d), (e), (f) and (g) of the definition of ***entity*** in the Digital ID Act, and is also approved as a participating relying party to provide, or to provide access to, one or more services within the AGDIS.

1.91. Third, a function of the transferring entity that includes the provision of the approved services is, or is reasonably expected to be, transferred to the receiving entity due to a MOG change. The effect of this provision is to enable receiving entities to submit a streamlined application when a MOG has occurred, or in anticipation of a pending MOG change as soon as it is announced, e.g. through a government announcement.

1.92. As receiving entities will only provide services after the MOG changes take effect, there is a risk that the receiving entity's application will not be considered and processed until after the MOG change occurs. This may result in the receiving entity not having the requisite approval to provide the services after the MOG change. As MOG changes commonly involve a delay between announcement and implementation, the provision enables applications before the MOG change takes effect. This maximises the time available for the Digital ID Regulator to assess and approve the application before the date that the MOG changes take effect.

1.93. Fourth, the application is for approval to provide, or to provide access to, one or more of the approved services of the transferring entity. While approval to participate broadly enables an entity to participate in the AGDIS, the conditions attached to that approval specify the particular services the relying party is authorised to provide or to provide access to.

1.94. Conditions relating to services may be imposed either on application by the relying party or on the Digital ID Regulator's own initiative, as provided for in subsection 64(3) of the Digital ID Act. Accordingly, a streamlined application will necessarily include a request for a condition under subsection 64(3), to authorise the provision of the same service/s delivered by the transferring entity.

1.95. The effect and purpose of the definition of streamlined application is to confine its operation to the limited circumstances of a Commonwealth, State or Territory government MOG change. In these circumstances the nature of the services, governance structures, and risk environment is likely to remain substantially unchanged. As a result, the full application requirements may not be necessary. It remains open for the Digital ID Regulator to exercise any of its powers under the Digital ID Act, such as those related to seeking further information from the applicant.

1.96. "Machinery of government" is not defined in the Amendment Rules and it is intended for the ordinary meaning of the term to apply. MOG is a well-established concept in Australian government administration and it is understood to refer to changes in the structure or responsibilities of government entities, such as the transfer of functions between those entities. It is envisaged that the streamlined applications will apply in circumstances where the provision of relevant services within the AGDIS will be transferred to another government entity.

1.97. Streamlined applications are limited to an applicant seeking to participate in the AGDIS as a participating relying party. These amendments do not affect accredited entities (as defined in section 9 of the Digital ID Act) and they are not able to make streamlined applications. Accredited entities have additional, privacy, security, usability and other compliance obligations given their role in providing digital ID services.

1.98. An entity cannot provide services (or access to services) in the AGDIS before its participation start day, as set out in paragraph 64(1)(d) of the Digital ID Act. This date is determined by the Digital ID Regulator and specified in the participation approval notice under paragraph 62(6)(d). Entities expecting to receive a function that delivers AGDIS services due to a MOG change, should apply for approval and seek a condition authorising provision of the service/s before acquiring the relevant function. The approval may be granted to take effect from the date the MOG change occurs. Entities that do not yet exist cannot apply as they are not an entity under the Digital ID Act.

1.99. MOG changes may introduce considerations around service continuity, particularly where a new entity is established. The Digital ID Act allows for multiple entities to concurrently hold approval to provide the same service/s within the AGDIS. If both the transferring and receiving entities intend to operate within the AGDIS, prior to connecting and delivering services each entity must be approved to participate in the AGDIS with a condition to provide the same service/s (to satisfy the requirements for providing or receiving services within the AGDIS as set out in item 4 of subsection 59(1)). The Digital ID Regulator is responsible for determining whether approvals for the same service/s may be granted to multiple entities.

Item 3 - Before subrule 2.2(1)

1.100. Item 3 inserts new subrule 2.2(1A) before subrule 2.2(1).

1.101. New subrule 2.2(1A) provides that this rule does not apply in relation to a streamlined application.

1.102. In considering whether to approve an entity to participate in the AGDIS, paragraph 62(1)(e) of the Digital ID Act relevantly requires the Digital ID Regulator to be satisfied

that it is appropriate to approve the entity to participate in the system. In making this assessment, the Digital ID Regulator may have regard to if an applicant is a fit and proper person under subsection 62(2) of the Digital ID Act.

1.103. Section 12 of the Digital ID Act relevantly provides that if the Digital ID Regulator does have regard to whether the entity is a fit and proper person, it:

- must have regard to the matters (if any) specified in the Digital ID Rules; and
- may have regard to any other matters the Digital ID Regulator considers relevant.

1.104. Rule 2.2 outlines the mandatory relevant matters to which the Digital ID Regulator must have regard if considering whether an entity is a fit and proper person. These matters broadly include the history of regulatory contravention, corporate disqualification, criminal convictions and privacy breaches involving the entity's key personnel.

1.105. The effect of proposed new subrule 2.2(1A) is to enable the Digital ID Regulator to not consider these mandatory matters in the context of a streamlined application, because following a MOG change the receiving entity's risk profile is often substantially unchanged.

Item 4 - After rule 2.2

1.106. Item 4 inserts a new rule 2.3 'Mandatory relevant matters—government entities affected by a machinery of government change'.

2.3 Mandatory relevant matters—government entities affected by a machinery of government change

1.107. Broadly, new rule 2.3 sets out the mandatory relevant matters which the Digital ID Regulator must have regard to in determining whether a receiving entity, as described in subrule 1.4(2) and 1.5, is a fit and proper person.

1.108. Subrule 2.3(1) provides that this rule applies in relation to a streamlined application. The effect of this provision is to limit the application of the matters in this provision to a streamlined application.

1.109. Subrule 2.3(2) provides that in considering whether the receiving entity is a fit and proper person, the Digital ID Regulator must have regard to whether the approval to participate held by the transferring entity has ever been suspended or revoked.

1.110. New subrule 2.3(3) mirrors paragraph 2.2(1)(j) of the fit and proper considerations, reflecting that if a post-MOG receiving entity has substantially similar processes and personnel within the business unit/s providing the approved service/s, and their risk profile remains unchanged, the most relevant fit and proper consideration remains the previous and current status of the transferring entity's approval. Where an entity has previously had its approval suspended or revoked, this may indicate weaknesses in its internal processes and may require greater scrutiny.

1.111. If the Digital ID Regulator chooses to have regard to whether the entity is a fit and proper person, it can rely on paragraph 12(b) to have regard to any other matters it considers relevant to whether the entity is a fit and proper person.

Item 5 - Rule 3.1 (after the heading)

1.112. Item 5 inserts a new subrule 3.1(1) after the heading.

1.113. The effect of item 5 is to exclude streamlined applications from the mandatory requirements in Part 1, Chapter 3 of the Digital ID Rules.

1.114. Rule 3.1 generally provides that Part 1 of Chapter 3 sets out the additional requirements that must be met before the Digital ID Regulator may approve an entity to participate in the AGDIS. Rules 3.2 and 3.3 broadly set out requirements for relying parties seeking approval to participate in the AGDIS, including System Administrator notification procedures, risk assessments, cybersecurity and digital ID fraud management plans, and disaster recovery and business continuity plans.

1.115. Excluding streamlined applications from the requirements in rules 3.2 and 3.3 acknowledges that the assessments and documentation required by rules 3.2 and 3.3 have been previously created and may not need to be reassessed in the circumstances of a MOG change.

1.116. It remains open for the Digital ID Regulator to exercise any of its powers under the Digital ID Act to determine whether the entity should be approved to participate in the AGDIS. For example, subsection 142(1) of the Digital ID Act relevantly provides that the Digital ID Regulator may require the applicant to provide such further information or documents in relation to the application as the Digital ID Regulator reasonably requires.

Item 6 - Rule 3.1

1.117. Item 6 numbers the existing text of Rule 3.1 as subrule (2), to make space for the new subrule (1) immediately before it. Item 6 is a consequential amendment only.

Schedule 3—Authorised entities for trustmarks

Item 1 – Paragraph 5.4(2)(c)

1.118. Item 1 omits 'and' from the end of paragraph 5.4(2)(c) of the Digital ID Rules.

1.119. This amendment is consequential to the amendment in Item 2 of Schedule *Digital ID Amendment (Redress Framework and Other Measures) Rules 2025* which adds a new paragraph at the end of subrule 5.4(2).

Item 2 – At the end of subrule 5.4(2)

1.120. Item 2 adds a new paragraph at the end of subrule 5.4(2) of the Digital ID Rules.

1.121. Broadly, this Item adds the Data Standards Chair to the list of entities authorised to use or display the Digital ID Accreditation Trustmark (digital ID trustmark) in connection with their statutory functions.

1.122. Chapter 8 of the Digital ID Act establishes the use and regulation of digital ID trustmarks. Section 116 of the Digital ID Act provides a simplified outline of Chapter 8, generally providing that the Digital ID Rules may set out marks, symbols, logos or designs (called digital ID trustmarks) that may or must be used by accredited entities and participating relying parties.

1.123. Subsection 118(1) of the Digital ID Act relevantly provides that an entity is authorised to use the digital ID trustmark if the entity is permitted or required by the Digital ID Rules, and the entity complies with any conditions prescribed in relation to the use or display of the digital ID trustmark.

1.124. Chapter 5 of the Digital ID Rules provides for the digital ID trustmarks. Rule 5.1 generally provides that Chapter 5 specifies the digital ID trustmark that may be used, and the conditions in relation to the use or display of that digital ID trustmark, by:

- an accredited entity, for the purposes of paragraph 117(1) of the Digital ID Act (subrule 5.1(1)); and
- an entity specified in rule 5.4 (***authorised entity***) for the purposes of paragraph 168(1)(b) of the Digital ID Act (subrule 5.1(2)).

1.125. Rule 5.2 provides that the digital ID trustmark specified in item of Schedule 1 is known as the ***Digital ID Accreditation Trustmark*** and may be used by an accredited entity and an authorised entity.

1.126. The purpose of the Digital ID Accreditation Trustmark is to be a visual indicator to signal that an entity is an accredited entity, for the purposes of, and in accordance with conditions, set out in Rule 5.3. This is designed to promote confidence in accredited services amongst Australian consumers and businesses.

1.127. The Digital ID Act also enables the Digital ID Rules to provide for other trustmarks, such as for participants in the Australian Government Digital ID System. However, the Digital ID Accreditation Trustmark is currently the only digital ID trustmark.

1.128. In general terms, the effect of rule 5.4 is to prescribe the conditions for which an authorised entity can use or display the digital ID trustmark.

1.129. Subrule 5.4(2) provides a list of entities that are authorised to use or display the digital ID trustmark. These entities are not accredited entities; they are government entities that are authorised to use the trustmark in connection with their statutory functions and other purposes as outlined in 5.4(3) relating to education about or promoting the objects of the Digital ID Act.

1.130. Subrule 5.4(2) currently includes the following authorised entities: the Digital ID Regulator, the System Administrator, the Information Commissioner, and the Secretary of the Department of Finance.

1.131. This amendment adds the Data Standards Chair to that list, which has the effect of enabling the Data Standards Chair to use or display the digital ID trustmark in accordance with the purposes outlined in subrule 5.4(3).

1.132. These purposes relate to the use or display of the digital ID trustmark in connection with the entity's statutory functions under the Digital ID Act and for other purposes relating to education about or promoting the objects of the Act.

1.133. The Data Standards Chair is a statutory role established under section 101 of the Digital ID Act. Generally, under section 102 of the Digital ID Act, the Data Standards Chair is responsible for making and reviewing Digital ID Data Standards, which provide for the technical and operational requirements of the Australian Government Digital ID system, and the accreditation scheme.

1.134. Prescribing the Chair as an authorised entity to use the digital ID trustmark ensures that the trustmark can be used as part of materials that may be developed by the Chair to support their performance of their statutory functions.

1.135. The effect of this amendment does not extend the Chair's scope to generally authorise the Chair to use the digital ID trustmark for purposes beyond those outlined in subrule 5.4(3). Care must be taken to ensure that use of the trustmark is limited to what is authorised under section 118 of the Act.

1.136. Like other authorised entities listed in subrule 5.4(2), use of this trustmark by the Chair is not intended to imply that the Chair has been accredited or operates an accredited service.

Schedule 4—Reportable incidents

Item 1 – At the end of rule 4.2

1.137. This amendment introduces subrules (7), (8) and (9) at the end of rule 4.2 of the Digital ID Rules.

1.138. Rule 4.2 broadly outlines the obligations on entities participating in the AGDIS (including those whose approval is suspended or revoked) to notify the System Administrator of any cyber security or digital ID fraud incidents that occur or are reasonably suspected to have occurred in relation to accredited services.

1.139. Subrule 4.2(3) broadly sets out the information that must be included in notifications. Subrule 4.2(4) generally provides that notifications must be made as soon as practicable and no later than one business day after the entity becomes aware of the incident.

1.140. New subrule 4.2(7) relevantly provides that if the System Administrator receives a notification under subrule 4.2(2), the System Administrator may direct any entity of a kind mentioned in subrule 4.2(1) who has interacted with a digital ID affected by the incident to conduct an investigation into the incident. This directions power operates alongside the System Administrator's powers under the Digital ID Act.

1.141. The purpose of this provision is to increase efficiencies for the System Administrator in exercising its functions under the Digital ID Act. In particular, this supports the System Administrator in managing digital ID fraud incidents and cyber security incidents involving entities participating in the AGDIS consistently with its function under paragraph 95(e) of the Digital ID Act.

1.142. New subrule 4.2(8) sets out procedural requirements for the entity once directed to conduct an investigation. Specifically, that entity must begin the investigation as soon as reasonably practicable and must provide the System Administrator with a summary of the findings of the investigation as soon as reasonably practicable after the investigation is complete.

1.143. New subrule 4.2(9) relevantly provides that if an investigation exceeds a period of 28 days, the entity must provide the System Administrator with updates on the progress of the investigation immediately after the 28 days and at least once every 28 days until the investigation is complete. The intent of this subrule is to provide the System Administrator with oversight of the progress of ongoing investigations and to provide a touch point for entities undertaking investigations.

Schedule 5—Application, saving and transitional provisions

Item 1 – After Chapter 6

1.144. This amendment introduces 'Chapter 7 – Application, saving and transitional provisions' after Chapter 6 in the Digital ID Rules, and new rule 7.1.

7.1 Application of amendments made by the Digital ID Amendment (Redress Framework and Other Measures) Rules 2025

1.145. Rule 7.1 sets out the application provisions for the amendments made by the Amendment Rules.

1.146. Subrule 7.1(1) defines "amending Rules" as the *Digital ID Amendment (Redress Framework and Other Measures) Rules 2025* and "commencement day" as the day on which those rules commence.

1.147. Subrule 7.1(2) provides that new rules 4A.2 and 4A.3 apply in relation to incidents that occur, or are reasonably suspected of having occurred, on or after the commencement day.

1.148. Subrule 7.1(3) provides that new rules 4A.7 and 4A.8 apply to entities to which new Chapter 4A applies on and after the end of the period of 6 months beginning on the commencement day. A 6-month transition period provides entities with sufficient time to develop and publish such policies, noting that the new requirements do not require the entity to develop a standalone complaints policy for digital ID incidents only. This also acknowledges existing requirements under the Accreditation Rules, including for entities to maintain processes and procedures relating to incidents, such as subrules 4.16(3) and 4.34(3) of the Accreditation Rules.

1.149. Subrule 7.1(4) provides that new subrules 4.2(7) and (8) apply in relation to notifications received on or after the commencement day.