Digital ID Rules 2024

I, Katy Gallagher, Minister for Finance, make the following rules.

Dated

DRAFT ONLY—NOT FOR SIGNATURE
Katy Gallagher
Minister for Finance

Contents

Part 1—Preliminary

1 Name

These rules are the *Digital ID Rules 2024*.

2 Commencement

(1) Each provision of these rules specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information		
Column 1	**Colum 2**	**Column 3**
Provisions	**Commencement**	**Date/Details**
1. The whole of these rules	The time at which the *Digital ID Act 2023* commences.	

Note: This table relates only to the provisions of this instrument as originally made. It will not be amended to deal with any later amendments of this instrument.

(2) Any information in column 3 of the table is not part of these rules. Information may be inserted in this column, or information in it may be edited, in any published version of these rules.

3 Authority

These rules are made under section 158 of the *Digital ID Act 2024* and for the purposes of the provisions in the Act in which the term 'Digital ID Rules' occurs.

4 Definitions

Note: Some expressions used in these rules are defined in the Act, including:

- accredited entity
- accredited attribute service provider
- accredited identity exchange provider
- accredited identity service provider
- accredited service
- affected entity
- attribute
- attribute service provider
- Australia
- Australian Government Digital ID System
- biometric information
- cyber security incident
- digital ID
- digital ID fraud incident
- Digital ID Regulator
- Digital ID system

- enforcement body
- participating relying party
- personal information
- reviewable decision

(1) In these rules:

Accreditation rules means the Digital ID Accreditation Rules made under the Act.

associated person, of an entity, means any of the following:

(a) a person who:

(i) makes, or participates in making, decisions that affect:

(A) the entity's management of its DI data environment; or

(B) for a participating relying party—the entity's functions when operating in the Australian Government Digital ID System; or

(ii) has the capacity to significantly affect:

(A) the entity's management of its DI data environment; or

(B) for a participating relying party—the entity's functions when operating in the Australian Government Digital ID System; or

(iii) who would be a person mentioned in subparagraphs (i) or (ii) if the entity was an accredited entity or held an approval to participate in the Australian Government Digital ID System; and

(b) if the entity is a body corporate—a person who:

(i) is an associate (within the meaning of the *Corporations Act 2001*) of the entity; or

(ii) is an associated entity (within the meaning of the *Corporations Act 2001*) of the entity.

banning order has the same meaning as in the *Corporations Act 2001*.

digital ID information has the same meaning as in the Accreditation Rules.

participating entity means an entity that holds an approval to participate in the Australian Government Digital ID System.

Privacy Act means the *Privacy Act 1988*.

reportable incident means an incident of a kind referred to in Part 4.

reportable incident requirement means a requirement in these rules in respect of a reportable incident.

Part 2—Fit and proper person considerations

5 Mandatory relevant matters

(1) For the purposes of section 12 of the Act, in having regard to whether an entity is a fit and proper person, the Digital ID Regulator must have regard to:

(a) whether the entity, or an associated person of the entity, has, within the previous 10 years, been convicted or found guilty of:

(i) a serious criminal offence; or

(ii) an offence of dishonesty;

against any law of the Commonwealth or of a State or Territory, or a law of a foreign jurisdiction;

(b) whether the entity, or an associated person of the entity, has been found to have contravened:

(i) a law relevant to the management of its DI data environment; or

(ii) a similar law of a foreign jurisdiction;

(c) whether the entity, or an associated person of the entity, has been the subject of:

(i) a determination under paragraph 52(1)(b), or any of paragraph 52(1A)(a), (b), (c) or (d), of the Privacy Act; or

(ii) a finding or determination of a similar nature under a similar law of a foreign jurisdiction;

(d) if the entity is a body corporate—whether any of the directors (within the meaning of the *Corporations Act 2001*) of the entity, or of an associated person of the entity:

(i) has been disqualified from managing corporations; or

(ii) is subject to a banning order;

(e) whether the entity, or an associated person of the entity, has a history of insolvency or bankruptcy;

(f) whether the entity, or an associated person of the entity, has been the subject of a determination made under an external dispute resolution scheme that:

(i) included a requirement to pay compensation; and

(ii) was, at the time the determination was made:

(A) recognised under the Privacy Act; or

(B) a recognised external dispute resolution scheme,

being a determination that included a requirement to pay monetary compensation;

(g) if the entity has made an application for approval to participate in the Australian Government Digital ID System or for accreditation as an accredited entity—whether the application was refused;

(h) if the entity is or has been accredited as an accredited entity—whether the accreditation is or has been suspended or revoked;

(j) whether the entity:

(i) has made a false or misleading statement in an application under the Act; or

(ii) has given false or misleading information, documents or evidence to the Digital ID Regulator.

(2) Subrule (1) does not affect the operation of Part VIIC of the *Crimes Act 1914* or a corresponding provision of an Australian or a law of a foreign country.

Note: Part VIIC of the *Crimes Act 1914* includes provisions that, in certain circumstances, relieve persons from the requirement to disclose spent convictions and require persons aware of such convictions to disregard them.

(3) In this rule:

serious criminal offence means an offence for which, if the act or omission had taken place in the Jervis Bay Territory, a person would have been liable, on first conviction, to imprisonment for a period of not less than 5 years.

Note: Jervis Bay Territory is mentioned because it is a jurisdiction in which the Commonwealth has control over the criminal law.

Part 3—Participation in the Australian Government Digital ID System

6 Applications for approval to participate—all entities

(1) For the purposes of paragraph 59(1)(f) of the Act, an applicant for approval to participate in the Australian Government Digital ID System must meet the requirements in this rule.

(2) The entity must have effective procedures to notify the Digital ID Regulator promptly of:

(a) a proposed significant change to its information technology system that interacts with the Australian Government Digital ID System, where the change which will, or can reasonably be expected to have a material effect on the operation of the Australian Government Digital ID System, including any degradation of or loss of functionality within the System; and

(b) planned or unexpected outages or downtime affecting the entity's information technology system which will affect, or has affected, access by any other entity to the Australian Government Digital ID System.

7 Applications for approval to participate—relying parties

(1) For the purposes of paragraph 59(1)(f) of the Act, a relying party applying for approval to participate in the Australian Government Digital ID System must meet the requirements in this rule.

(2) The entity must have:

(a) a written plan for testing (within periods and at intervals specified in the plan) the interoperability of its information technology system within the Australian Government Digital ID System;

(b) conducted a risk assessment to identify, evaluate and manage the risks of a cyber security incident occurring within its information technology system that will operate within the Australian Government Digital ID System if the relying party is approved to participate;

(c) written processes and procedures set out in a fraud management plan approved by the entity's governing body:

(i) to investigate digital ID fraud incidents, including incidents notified to it by the Digital ID Regulator; and

(ii) to prevent, identify and investigate unauthorised access, including by the entity's personnel and contractors, to personal information which will be collected by the relying party if it is approved to participate; and

(d) a business continuity plan approved by the entity's governing body that addresses at least the following:

(i) disaster recovery procedures;

(ii) continuity procedures for critical functions of its information technology system;

(iii) regular reviews of the plan, but at least once a year.

8 Conditions on approval to participate

For subsection 62(6) of the Act, the approval of an entity described in an item of the following table is subject to the condition described in that item.

Item	Entity	Condition
1	Participating relying party	The entity must notify the Digital ID Regulator of a proposed change to its contact details no later than 28 days before the change takes effect.

9 Statutory contract—intellectual property rights

(1) For the purposes of paragraph 80(1)(d) of the Act, it is a requirement that an accredited entity that is a party to the statutory contract (the ***first party***) warrants to other parties to the contract that the use by a person mentioned in subrule (2), of an item provided or made available by the first party for use within the Australian Government Digital ID System does not infringe the intellectual property rights of the first party or any person not a party to the statutory contract.

(2) The persons are:
- (a) the other party to the statutory contract;
- (b) any other participating entity; and
- (c) a contractor to a person mentioned in paragraph (a) or (b).

(3) The reference in subrule (1) to use of an item is a reference to its use within the Australian Government Digital ID System.

(4) In this rule:

intellectual property rights includes moral rights as defined in the *Copyright Act 1968*.

10 Holding etc. information outside Australia

(1) This rule is made for the purposes of section 73 of the Act and applies to:
- (a) an accredited entity that holds an approval to participate in the Australian Government Digital ID System; and
- (b) an accredited entity whose approval to participate in the Australian Government Digital ID System is suspended or has been revoked.

(2) In this rule:

system information means information generated, collected, held or stored by the entity in relation to the Australian Government Digital ID System.

(3) The entity must not do any of the following, or cause or permit another person to do any of the following:
- (a) hold, store or handle system information at a place outside Australia; or
- (b) transfer system information to a place outside Australia for storage or handling,

unless the entity holds an exemption granted under subrule (5) in respect of the holding, storage, handling or transferring of the system information and the entity complies with any conditions on the exemption.

(4) Subrule (3) does not apply in relation to:
  (a) a request by the individual to whom the system information relates, being a request made from a place outside Australia; or
  (b) transferring information to:
    (i) verify the identity of an individual; or
    (ii) authenticate the digital ID of, or information about, an individual,
    where the verification or authentication is to occur at the place outside Australia.

(5) On application by an entity mentioned in subrule (1), the Minister may grant, in writing, the entity an exemption in respect of the holding, storage, handling or transferring of the system information at a specified place outside Australia.

Note: See Part 5 of Chapter 8 of the Act for matters relating to applications.

(6) Without limiting what an application for an exemption must include, it must include or be accompanied by information addressing:
  (a) whether the law of the specified place has the effect mentioned in paragraph (8)(a);
  (b) whether there is a scheme in effect in the specified place that has the effect mentioned in paragraph (8)(a); and
  (c) whether there are mechanisms of the kind mentioned in paragraph (8)(b) in the specified place.

(7) In considering whether to grant an exemption to an entity:
  (a) the matters that the Minister must consider include:
    (i) a risk assessment plan provided by the entity;
    (ii) a privacy impact assessment provided by the entity, so far as it relates to personal information that may be disclosed under the proposed exemption; and
    (ii) the effectiveness of the entity's protective security (including security governance, information security, personnel security and physical security) and fraud control arrangements; and
  (b) the matters that the Minister may consider include whether the technology required by the entity is available in Australia or is available to the entity in Australia.

(8) The Minister must not grant an exemption to an entity in relation to system information unless the Minister is satisfied that:
  (a) the person that will hold, store or handle the system information at a place outside Australia is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles set out in Schedule 1 of the Privacy Act protect the information; and
  (b) there are mechanisms that the individual to whom the information relates can access to take action to enforce that protection of the law or binding scheme.

Review of decisions

(9) For subsection 131(2) of the Act:

(a) a decision made under subrule (5) to refuse to grant an exemption to an entity is a reviewable decision and the entity that applied for the exemption is the affected entity;

(b) a decision under subrule (5) to impose conditions on an exemption granted to an entity is a reviewable decision and the entity that applied for the exemption is the affected entity; and

(c) a decision to revoke an exemption is a reviewable decision and the entity to which the exemption relates is the affected entity.

Note: The Minister may revoke the exemption: see subsection 33(3) of the *Acts Interpretation Act 1901*.

11 Interoperability obligation

(1) This rule is made for the purposes of section 75 of the Act.

Circumstances in which the interoperability obligation applies to a participating relying party

(2) The interoperability obligation described in paragraph 75(2)(a) of the Act, applies to a participating relying party where more than one accredited entity service provider:

(a) is approved to participate in the Australian Government Digital ID System;

(b) is accredited to provide its services at the identity proofing level and any authentication level sought by the participating relying party; and

(c) is required to provide its services to the participating relying party.

Note 1: The interoperability obligation specified in paragraph 75(2)(a) of the Act means that a participating relying party must permit an individual to choose which of the accredited identity service providers provides the service to the participating relying party.

Note 2: Conditions may be imposed on the accreditation of an accredited identity service provider that specify the identity proofing levels or types of authenticators that the entity can provide (see subsection 18(5) of the Act).

Circumstances in which the interoperability obligation applies to an accredited entity

(3) The interoperability obligation described in paragraph 75(2)(b) of the Act, applies to all accredited entities participating in the Australian Government Digital ID System.

Note: The interoperability obligation specified in paragraph 75(2)(b) of the Act means that an accredited entity participating in the Australian Government Digital ID System must provide the services for which it is accredited to another accredited entity or a participating relying party.

Exemption from interoperability obligation

(4) On application by a participating entity, the Minister may grant, in writing, the entity an exemption from the interoperability obligation if the Minister considers it appropriate to do so.

Note: See Part 5 of Chapter 8 of the Act for matters relating to applications.

(5) However, an accredited identity exchange provider cannot apply for, and must not be granted, an exemption from the interoperability obligation.

(6) The grounds on which the Minister may grant an exemption include the grounds specified in paragraph 75(3)(c) of the Act.

(7) An exemption granted to an entity may be subject to a condition and, if so, the entity must comply with the condition.

Review of decisions

(8) For subsection 131(2) of the Act:

(a) a decision under subsection (4) to refuse to grant an exemption to an entity is a reviewable decision and the entity that applied for the exemption is the affected entity;

(b) a decision under subsection (7) to impose, or not to impose a condition sought by the entity, is a reviewable decision and the entity to which the condition applies is the affected entity; and

(c) a decision to revoke an exemption is a reviewable decision and the entity to which the exemption relates is the affected entity.

Note: The Minister may revoke the exemption: see subsection 33(3) of the *Acts Interpretation Act 1901*.

Part 4—Reportable incidents

12 Cyber security incidents

(1) The arrangements described in this rule are prescribed for the purposes of section 74(1) of the Act.

(2) The arrangements described in this rule apply to:
  (a) a participating entity;
  (b) an entity whose approval to participate is suspended; and
  (c) an entity whose approval to participate has been revoked, but only in respect of incidents that occurred while the entity was participating in the Australian Government Digital ID System .

(3) The entity must notify the Digital ID Regulator, in accordance with this rule, of any cyber security incidents that occur in relation to:
  (a) the entity's accredited services provided within the Australian Government Digital ID System; or
  (b) for a participating relying party—services received by the entity within that System.

(4) A notification by an entity of an incident must include the following information:
  (a) the entity's name;
  (b) the contact details of the entity;
  (c) if the entity is accredited as more than one kind of accredited entity—the service affected by the incident;
  (d) a description of the incident;
  (e) the following details of the incident, so far as they are known to the entity:
    (i) the date and time of the incident;
    (ii) the date on which the entity became aware of the incident;
    (iii) the method or source of detection of the incident;
    (iv) the severity of the incident;
    (v) whether the incident has been resolved; and
    (vi) if the incident has been resolved—how it was resolved and how long the entity took to resolve it;
  (f) if the entity is aware of similar incidents within the previous 12 months—the number of those incidents;
  (g) if the entity is an accredited identity service provider:
    (i) the digital ID or identities affected by the incident; and
    (ii) the attributes and authenticator of each of those identities affected by the incident;
  (h) for each individual whose digital ID is affected by the incident, whether the individual has been informed of the incident and, if so, when;
  (i) any relevant identity proofing level and authentication level and, if an individual's digital ID has been re-proofed because of the incident, the date that happened;
  (j) the measures that the entity has taken and plans to take to deal with the incident, including action taken or to be taken to reduce risk to the services

the entity provides or receives in the Australian Government Digital ID System;

(k) whether the incident has been referred to an enforcement body and, if so, to which body and when; and

(l) if the entity is a participating relying party—the identifier issued to the relying party in relation to each individual associated with the incident.

(5) A notification of an incident required by this rule must be made as soon as practicable after, and in any event no later than 24 hours after, the entity becomes aware of the incident or a suspected incident.

(6) A notification of an incident required by this section may be given orally. However, if it is given orally, a written notification must be given within 3 working days after the oral notification.

(7) If the entity is not able to provide some or all of the information required by subsection (4) in relation to an incident, so that it is not practicable for the entity to comply fully with that subsection within the period specified in subsection (5) or (6), the entity is taken to comply with subsection (4) if:

(a) it takes reasonable steps to obtain the missing information as soon as possible;

(b) it provides an interim notification by the time required by subsection (5) or (6) with as much of the required information as is available to it;

(c) at intervals of no longer than 48 hours thereafter—it notifies additional required information as is available to it; and

(d) the entity completes the notification as soon as practicable after making the interim notifications.

13 Digital ID fraud incidents

(1) The arrangements described in this section are prescribed for subsection 74(1) of the Act.

(2) The arrangements described in this section apply to:

(a) a participating entity;

(b) an entity whose approval to participate is suspended; and

(c) an entity whose approval to participate has been revoked, but only in respect of incidents that occurred while the entity was participating in the Australian Government Digital ID System.

(3) The entity must notify the Digital ID Regulator, in accordance with this section, of the following kinds of incidents digital ID fraud incidents in relation to:

(a) for an accredited entity (when the incident occurred)—its accredited services; or

(b) for a participating relying party (when the incident occurred)— services received by the entity within that System..

(4) A notification by an entity of an incident must include the following information:

(a) the entity's name;

(b) the contact details of the entity;

(c) if the entity is accredited as more than one kind of accredited entity—the service affected by the incident;
(d) a description of the incident;
(e) the following details of the incident, so far as they are known to the entity:
(i) the date and time of the incident;
(ii) the date on which the entity became aware of the incident;
(iii) the method or source of detection of the incident;
(iv) the severity of the incident;
(v) whether the incident has been resolved;
(vi) if the incident has been resolved—how it was resolved and how long the entity took to resolve it;
(f) if the entity is aware of similar incidents within the previous 12 months—the number of those incidents;
(g) if the entity is an accredited identity service provider;
(i) the digital ID or identities affected by the incident; and
(ii) the attributes and authenticators of each of those identities; and
(h) for each individual whose digital ID is affected by the incident, whether the individual has been informed of the incident and, if so, when;
(i) any relevant identity proofing level and authentication level and, if an individual's digital ID has been re-proofed because of the incident, the date that happened;
(j) the measures that the entity has taken and plans to take to deal with the incident, including action taken or to be taken to reduce risk to services the entity provides or receives in the Australian Government Digital ID System;
(k) whether the incident has been referred to an enforcement body and, if so, to which body and when; and
(l) if the entity is a participating relying party—the identifier issued to the relying party in relation to each individual associated with the incident.

(5) A notification of an incident required by this rule must be made as soon as practicable after, and in any event no later than 24 hours after, the entity becomes aware of the incident.

(6) A notification of an incident required by this rule may be given orally. However, if it is given orally, a written notification must be given within 3 working days after the oral notification.

(7) If the entity is not able to provide some or all of the information required by subsection (4) in relation to an incident, so that it is not practicable for the entity to comply fully with that subsection within the period specified in subsection (5) or (6), the entity is taken to comply with subsection (4) if:
(a) it takes reasonable steps to obtain the missing information as soon as possible;
(b) it provides an interim notification by the time required by subsection (5) or (6) with as much of the required information as is available to it;
(c) at intervals of no longer than 48 hours thereafter—it notifies additional required information as is available to it; and

(d) the entity completes the notification as soon as practicable after making the interim notifications.

14 Changes in control of corporations

(1) The arrangements described in this rule are prescribed for subsection 74(1) of the Act.

(2) This section applies to:

(a) a participating entity that is a corporation; and

(b) an entity that is a corporation whose approval to participate is suspended,

but does not apply to a corporation that is controlled by the Commonwealth, a State or Territory or an authority of a State or Territory.

(3) The entity must notify the Digital ID Regulator, in accordance with this rule, of a change in control (within the meaning of section 910B of the *Corporations Act 2001*), or a proposed change of control, of the entity.

(4) A notification of a change in control, or a proposed change of control, of an entity must include the following information:

(a) the entity's name;

(b) the contact details for the entity;

(c) the following details in respect of each entity that, through the change or proposed change in control of the entity, has started or would start to control the entity (***incoming entity***):

(i) the name of the incoming entity;

(ii) the incoming entity's ABN or ARBN;

(iii) the address of the incoming entity's principal place of business;

(iv) the other contact details of the incoming entity;

(v) if the incoming entity was incorporated outside Australia—the location of its incorporation and the address of its principal place of business in Australia;

(vi) the business name of the incoming entity;

(vii) the date on which the incoming entity was registered under the *Corporations Act 2001* or other law;

(viii) the names and director identification number of each of the directors and other officers of the incoming entity;

(ix) in respect of each subsidiary (as defined in section 9 of *Corporations Act 2001*) of the incoming entity—the information specified in subparagraphs (i) to (viii); and

(e) the date on which the change of control occurred or is proposed to occur.

(5) A notification required by this rule must be made:

(a) if the entity becomes aware of a proposal for the change in control before it occurs—within 72 hours after the entity becomes aware; or

(b) otherwise—within 72 hours after the change in control occurs.

(6) In this rule:

corporation has the meaning given in the *Corporations Act 2001*.

director has the meaning given in section 9 of the *Corporations Act 2001* and, for that purpose, ***body*** has the meaning given in that section.

officer has the meaning given in section 9 of the *Corporations Act 2001*.

subsidiary has the meaning given in section 9 of the *Corporations Act 2001*.

15 Change in contractor

(1) The arrangements described in this rule are:
  (a) prescribed for subsection 74(1) of the Act; and
  (b) apply to an accredited entity participating in the Australian Government Digital ID System.

(2) The entity must notify the Digital ID Regulator, in accordance with this rule, of the proposed engagement by the entity of a contractor to provide, on behalf of the entity, a service the entity is accredited to provide, or part of such a service, being a service provided within the Australian Government Digital ID System.

Note: The accredited entity's DI data environment will include details of contractors providing an accredited service on behalf of the accredited entity.

(3) A notification by an entity must include the following information:
  (a) if the entity is accredited as more than one kind of accredited entity—the service affected by the incident;
  (d) the following details in respect of the contractor (***incoming contractor***):
    (i) the name of the incoming contractor;
    (ii) the incoming contractor's ABN or ARBN;
    (iii) the address of the incoming contractor's principal place of business;
    (iv) if the incoming contractor was incorporated outside Australia—the location of its incorporation and the address of its principal place of business in Australia; and
    (v) any business names of the incoming contractor;
  (e) the date on which the engagement is proposed to start;
  (f) the date on which the engagement is proposed to end;
  (g) the names of each of the incoming contractor's key persons relevant to the engagement or proposed engagement;
  (h) a statement whether the contract under which the incoming contractor is or is proposed to be engaged requires the contractor to ensure that its activities under the contract do not result in the entity contravening the Act, these rules or the Accreditation rules.

(4) A notification required by this rule must be made no later than 28 days before the engagement is proposed to start.

(5) Subrule (1) does not apply if the proposal to engage the incoming contractor has previously been notified to the Digital ID Regulator, including in the entity's application for approval to participate.

16 Other events and circumstances

(1) The arrangements described in this rule are prescribed for subsection 74(1) of the Act and apply to:
  (a) a participating entity; and
  (b) an entity whose approval to participate is suspended.

(2) The entity must report the following matters to the Digital ID Regulator within 5 business days if any of the following occurs:
  (a) any material change in its circumstances that might affect its ability to comply with its obligations under the Act or the rules;
  (b) any matter that could be relevant to a decision as to whether the entity is, having regard to the fit and proper person criteria, a fit and proper person to be accredited, including matters involving an associated person of the entity; and
  (c) there is a change to, or the accredited entity becomes aware of an error in, any of the information provided to the Digital ID Regulator.

(3) A notification by an entity must include the following information:
  (a) the entity's name;
  (b) the contact details for the entity;
  (c) if the event or circumstance relates to an associated person of the entity—the name and contact details of the associated person; and
  (d) the details of the event or circumstance, including:
    (i) when it occurred or arose;
    (ii) its nature; and
    (iii) sufficient other details to enable the Digital ID Regulator to determine whether the Regulator should take any action in relation to the entity's approval to participate.

17 Reportable incidents—other digital ID systems

(1) The arrangements described in this rule are prescribed for subsection 74(1) of the Act and apply to:
  (a) an accredited entity which holds an approval to participate; and
  (b) an accredited entity whose approval to participate is suspended.

(2) If an entity proposes to use the information technology system through which it provides its accredited services to provide or receive services within a digital ID system other than the Australian Government Digital ID System , the entity must notify the Digital ID Regulator, in accordance with this rule, of the proposal.

(3) A notification by an entity must include the following information:
  (a) the entity's name;
  (b) the contact details for the entity;
  (c) if:
    (i) the entity is accredited as more than one kind of accredited entity; and

(ii) the service to be provided in or with the other digital ID system is of the same kind as a service it is accredited to provide in the Australian Government Digital ID System,

a description of the service to be provided in or with the other digital identity system;

(d) details of the entity providing or managing the other digital ID system;

(e) the nature of the proposed use of the other digital ID system;

(f) the likely effect of the entity's use of the other digital ID system or the digital ID on the levels of the entity's risk of a cyber security incident and risk of a digital ID fraud incident; and

(g) details of how the entity:

(i) will clearly distinguish information flows within the Australian Government Digital ID System from information flows within the other digital ID system;

(ii) will clearly distinguish between services provided in the Australian Government Digital ID System and those provided in or with the other digital ID system;

(iii) will ensure that information held by the entity for the purposes of the Australian Government Digital ID System will be separate from, and unable to be accessed for, or used in, the other digital ID system; and

(iv) will be able to meet its obligations under the Act and rules in respect of the services it is accredited to provide.

Example For subparagraphs (g)(i) and (ii), an information barrier.

(4) A notification required by this rule must be made no later than 28 days before the proposed use of the other digital ID system.

18 Capacity of the Australian Government Digital ID System

(1) The arrangements described in this rule are prescribed for subsection 74(1) of the Act and apply to a participating relying party.

(2) If:

(a) the number of transactions during a month, being transactions involving the participating relying party receiving services within the Australian Government Digital ID System, is 10% or more than the average number of such transactions occurring in each of the previous 6 months; and

(b) it is reasonable to expect that that level of use will continue or increase in the next 3 months,

the participating relying party must notify the Digital ID Regulator, in accordance with this rule, of the increase.

(3) A notification by a participating relying party must include the following information:

(a) its name;

(b) its contact details;

(c) the extent of the increase; and

(d) the reasons for the increase, so far as they are known to the participating relying party.

(4) The notification required by this rule must be made no later than 7 days after the end of the month concerned.

19 Digital ID Regulator may disclose information

(1) The Digital ID Regulator may give information notified to it under rules 12, 13 or 18 to the Minister or to a participating entity.

Note: These notifications relate to cyber security incidents, digital ID fraud incidents and increases in use of the Australian Government Digital ID System.

(2) If the Digital ID Regulator acquires information about a cyber security incident or a digital ID fraud incident otherwise than by a notification under rules 12 or 13, the Digital ID Regulator may give the information to a participating entity.

(3) The Digital ID Regulator may not give information under this rule unless it considers it appropriate to do so to protect the security, integrity or performance of the Australian Government Digital ID System.

(4) For the purposes of paragraph 74(2)(g) of the Act, a person or body to whom the Digital ID Regulator may disclose information under this rule is authorised to collect the information.

Part 5—Trustmarks

20 Digital ID trustmark

For section 113 of the Act, the trustmark specified in Schedule 1 must be displayed on each of accredited entity's website pages that a user accesses to enter or leave the digital ID system in which the entity operates.

21 This Part not to affect other rights

To avoid doubt, this Part does not affect any right arising under the *Trade Marks Act 1995* or the *Designs Act 2003* in respect of a digital ID trustmark or an element of a digital ID trustmark.

Part 6—Record-keeping

22 Record keeping by accredited entities and former accredited entities

(1) For subsection 129(3) of the Act, this rule prescribes records that entities must keep and the periods for which those records must be kept.

(2) For subsection 129(3) of the Act:

(a) in respect of prescribed information held by an accredited entity whose approval to participate is in force or has been suspended—the period that ends at the later of the following times is prescribed:

(i) 7 years after the date the record was created;

(ii) 7 years after the record was last used in the Australian Government Digital ID System for the purpose of providing a service that the entity is or was accredited to provide; and

(b) in respect of prescribed information held by an accredited entity whose approval to onboard has been revoked—the period that ends at the earlier of the following times is prescribed:

(i) the later of:

(A) 3 years after the record was created; and

(B) 3 years after the record was last used in the Australian Government Digital ID System for the purpose of providing a service that the entity was accredited to provide; and

(ii) if the record was created less than 7 years before the onboarding approval was revoked—7 years after the record was created.

(3) Subrules (1) and (2) do not relate to records that do not relate to information obtained by entities through the Australian Government Digital ID System.

(4) In this rule:

prescribed information means digital ID information that meets the logging requirements of rule 4.18 of the Accreditation Rules, and any additional logging requirements in Chapter 5 of the Accreditation Rules for the kind of accredited entity the entity is accredited as.