2022-2023

The Parliament of the
Commonwealth of Australia

HOUSE OF REPRESENTATIVES/THE SENATE

**EXPOSURE DRAFT**

# Digital ID Bill 2023

# No. , 2023

*(Finance)*

**A Bill for an Act to provide for the accreditation of entities in relation to digital IDs and to establish the Australian Government Digital ID System, and for related purposes**

# Contents

EXPOSURE DRAFT

# A Bill for an Act to provide for the accreditation of entities in relation to digital IDs and to establish the Australian Government Digital ID System, and for related purposes

The Parliament of Australia enacts:



EXPOSURE DRAFT

# Chapter 1—Introduction

# Part 1—Preliminary

## 1 Short title

This Act is the *Digital ID Act 2023*.

## 2 Commencement

(1) Each provision of this Act 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 | Column 2 | Column 3 |
|---|---|---|
| **Provisions** | **Commencement** | **Date/Details** |
| 1. The whole of the Act | A single day to be fixed by Proclamation.<br>However, if the provisions do not commence within the period of 6 months beginning on the day this Act receives the Royal Assent, they commence on the day after the end of that period. | |

Note: This table relates only to the provisions of this Act as originally enacted.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

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

Note: This table relates only to the provisions of this Act as originally enacted.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

## 3 Objects

(1) The objects of this Act are as follows:

(a) to provide individuals with a simple, inclusive and convenient method for verifying their identity in online transactions with government and businesses, while protecting their privacy and the security of their personal information;

(b) to promote economic advancement by building trust in digital ID services;

(c) to facilitate economic benefits for, and reduce burdens on, the Australian economy by encouraging the use of digital IDs and online services;

(d) to provide a digital ID system that will enable innovative digital sectors of the Australian economy to flourish.

(2) These objects are to be achieved by:

(a) enhancing the simplicity, safety, privacy and security of online transactions between individuals, government and businesses by:

(i) establishing a system of voluntary accreditation for entities participating in digital ID systems other than the Australian Government Digital ID System, ensuring such entities comply with the same strong privacy and integrity safeguards as those that apply to the Australian Government Digital ID System; and

(ii) improving the regulation and governance of providers of services within such systems; and

(b) establishing an Australian Government Digital ID System that is safe, secure, trusted, accessible, inclusive, easy to use, reliable and voluntary, and supported by strong privacy and integrity safeguards; and

(c) facilitating choice for individuals amongst providers of services within the Australian Government Digital ID System.

## 4 Simplified outline of this Act

*[to be drafted]*

## 5 Act binds the Crown

This Act binds the Crown in each of its capacities.

## 6 Extension to external Territories

This Act extends to every external Territory.

## 7 Extraterritorial operation

(1) This Act extends to acts, omissions, matters and things outside Australia.

Note: Geographical jurisdiction for civil penalty provisions is dealt with in section 152.

(2) This Act has effect in relation to acts, omissions, matters and things outside Australia subject to:

(a) the obligations of Australia under international law, including obligations under any international agreement binding on Australia; and

(b) any law of the Commonwealth giving effect to such an agreement.

## 8 Concurrent operation of State and Territory laws

This Act is not intended to exclude or limit the operation of a law of a State or Territory that is capable of operating concurrently with this Act.

# Part 2—Interpretation

## 9 Definitions

In this Act:

***Accreditation Rules*** means rules made under section 158 for the purposes of the provisions in which the term occurs.

***accredited attribute service provider*** means an attribute service provider that is accredited under section 15 as an accredited attribute service provider.

***accredited entity***: each of the following is an accredited entity:

(a) an accredited attribute service provider;

(b) an accredited identity exchange provider;

(c) an accredited identity service provider;

(d) if Accreditation Rules are made for the purposes of paragraph 14(1)(d)—an entity that is accredited to provide services of a kind prescribed by the Accreditation Rules for the purposes of that paragraph.

***accredited identity exchange provider*** means an identity exchange provider that is accredited under section 15 as an accredited identity exchange provider.

***accredited identity service provider*** means an identity service provider that is accredited under section 15 as an accredited identity service provider.

***accredited service***, of an accredited entity, means the services provided, or proposed to be provided, by the entity in the entity's capacity as a particular kind of accredited entity.

Note: Conditions may be imposed on an entity's accredited services, including specifying the manner in which such services must be provided or excluding specific services from the entity's accreditation altogether (see section 18).

Example: Acme Co is an accredited identity service provider. Under its conditions of accreditation, its accredited service is generating, managing, maintaining and verifying information relating to the identity of an individual. Its conditions exclude from its accreditation the provision of the following services:

(a) generating, binding, managing and distributing authenticators to an individual;

(b) binding, managing and distributing authenticators generated by an individual.

***adverse or qualified security assessment*** means an adverse security assessment, or a qualified security assessment, within the meaning of Part IV of the *Australian Security Intelligence Organisation Act 1979*.

***affected entity***: see section 131.

***AGDIS Register*** means the register kept under section 117.

***APP entity*** has the same meaning as in the *Privacy Act 1988*.

***APP-equivalent agreement***: see section 32.

***attribute*** of an individual: see section 10.

***attribute service provider*** means an entity that provides, or proposes to provide, a service that verifies and manages an attribute of an individual.

***Australia*** when used in a geographical sense, includes the external Territories.

***Australian entity*** means any of the following:

(a) an Australian citizen or a permanent resident of Australia;

(b) a body corporate incorporated by or under a law of the Commonwealth or a State or Territory;

(c) a Commonwealth entity, or a Commonwealth company, within the meaning of the *Public Governance, Performance and Accountability Act 2013*;

(d) a person or body that is an agency within the meaning of the *Freedom of Information Act 1982*;

(e) a body specified, or the person holding an office specified, in Part I of Schedule 2 to the *Freedom of Information Act 1982*;
(f) a department or authority of a State;
(g) a department or authority of a Territory;
(h) a partnership formed in Australia;
(i) a trust created in Australia;
(j) an unincorporated association that has its central management or control in Australia.

***Australian Government Digital ID System***: see subsection 55(2).

***authenticator*** means the technology for authenticating an individual's digital ID.

Note: Passwords and cryptographic keys are examples of authenticators.

***biometric information*** of an individual:
(a) means information about any measurable biological characteristic relating to an individual that could be used to identify the individual or verify the individual's identity; and
(b) includes biometric templates.

***civil penalty provision*** has the same meaning as in the Regulatory Powers Act.

***compliance assessment***: see section 126.

***cyber security incident*** means one or more acts, events or circumstances that involve:
(a) unauthorised access to, modification of or interference with a system, service or network; or
(b) an unauthorised attempt to gain access to, modify or interfere with a system, service or network; or
(c) unauthorised impairment of the availability, reliability, security or operation of a system, service or network; or
(d) an unauthorised attempt to impair the availability, reliability, security or operation of a system, service or network.

***digital ID*** of an individual means a distinct electronic representation of the individual that enables the individual to be sufficiently distinguished when interacting online with services.

***Digital ID Accredited Entities Register*** means the register kept under section 116.

***Digital ID Data Standards*** means the standards made under section 93.

***Digital ID Data Standards Chair*** means:

(a) if a person holds an appointment under section 99—that person; or

(b) otherwise—the Minister.

***digital ID fraud incident*** means an act, event or circumstance that:

(a) occurs in connection with:

(i) an accredited service of an accredited entity; or

(ii) a service that a participating relying party is approved to provide, or provide access to, within the Australian Government Digital ID System; and

(b) results in any of the following being, or suspected of being, compromised or rendered unreliable:

(i) the digital ID of an individual;

(ii) an attribute of an individual;

(iii) an authenticator relating to an individual;

(iv) a representation relating to an attribute of an individual;

(v) a representation relating to a digital ID of an individual.

***Digital ID Regulator***: see section 85.

***Digital ID Rules*** means the rules made under section 158 for the purposes of the provisions in which the term occurs.

***digital ID system*** means a federation of entities that facilitates, manages or relies on services that provide for either or both of the following in an online environment:

(a) the verification of the identity of individuals;

(b) the authentication of the digital ID of, or information associated with, individuals.

Note: Entities in the federation may include one or more relying parties, identity exchanges, identity service providers, attribute service providers and other kinds of service providers.

***digital ID trustmark***: see subsection 113(2).

***enforcement body*** has the same meaning as in the *Privacy Act 1988*.

***enforcement related activity*** has the same meaning as in the *Privacy Act 1988*.

***entity*** means any of the following:

(a) an individual;

(b) a body corporate;

(c) a Commonwealth entity, or a Commonwealth company, within the meaning of the *Public Governance, Performance and Accountability Act 2013*;

(d) a person or body that is an agency within the meaning of the *Freedom of Information Act 1982*;

(e) a body specified, or the person holding an office specified, in Part I of Schedule 2 to the *Freedom of Information Act 1982*;

(f) a department or authority of a State;

(g) a department or authority of a Territory;

(h) a partnership;

(i) an unincorporated association;

(j) a trust.

***entrusted person***: see subsection 88(2).

***identity exchange provider*** means an entity that provides, or proposes to provide, a service that conveys, manages and coordinates the flow of data or other information between participants in a digital ID system.

***identity service provider*** means an entity that provides, or proposes to provide, a service that:

(a) generates, manages, maintains or verifies information relating to the identity of an individual; and

(b) generates, binds, manages or distributes authenticators to an individual; and

(c) binds, manages or distributes authenticators generated by an individual.

***one-to-many matching***: see subsection 45(3).

***paid work*** means work for financial gain or reward (whether as an employee, a self-employed person or otherwise).

***participate***: an entity ***participates*** in the Australian Government Digital ID System at a particular time if, at that time:

(a) the entity holds an approval under section 59 to participate in the system; and

(b) either:

(i) the entity is directly connected to an accredited entity that is participating in the Australian Government Digital ID System; or

(ii) the entity is an accredited entity that is directly connected to a participating relying party.

***participating relying party***: a relying party is a ***participating relying party*** if:

(a) the relying party holds an approval under section 59 to participate in the Australian Government Digital ID System; and

(b) the participation start day for the relying party has arrived or passed.

***participation start day*** for an entity means the day notified to the entity by the Digital ID Regulator for the purposes of paragraph 59(6)(c) as the day on which the entity must begin to participate in the Australian Government Digital ID System.

***personal information***:

(a) means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(i) whether the information or opinion is true or not; and
(ii) whether the information or opinion is recorded in a material form or not; and

(b) to the extent not already covered by paragraph (a), includes an attribute of an individual.

***privacy impact assessment*** has the meaning given by subsection 33D(3) of the *Privacy Act 1988*.

***protected information***: see subsection 88(4).

***Regulatory Powers Act*** means the *Regulatory Powers (Standard Provisions) Act 2014*.

***relying party*** means an entity that relies, or seeks to rely, on an attribute of an individual that is provided by an accredited entity to:

(a) provide a service to the individual; or
(b) enable the individual to access a service.

***restricted attribute*** of an individual: see section 11.

***reviewable decision***: see section 131.

***Secretary*** means the Secretary of the Department.

***security***, other than in the following provisions, has its ordinary meaning:

(a) subparagraph 15(5)(c)(ii);
(b) subsection 16(1);
(c) subsection 16(2);
(d) subsection 18(4);
(e) paragraph 20(2)(b);
(f) paragraph 25(2)(d);
(g) paragraph 26(1)(d);
(h) paragraph 59(2)(a);
(i) subsection 60(1);
(j) subsection 60(2);
(k) subsection 62(4);

(l) paragraph 64(2)(b);
(m) paragraph 69(2)(d);
(n) paragraph 70(1)(c);
(o) subsection 131(3).

***shielded person*** means a person to whom one or more of the following paragraphs apply:

(a) the person has acquired or used an assumed identity under Part IAC of the *Crimes Act 1914* or a corresponding assumed identity law within the meaning of that Part;
(b) an authority for the person to acquire or use an assumed identity has been granted under that Part or such a law;
(c) a witness identity protection certificate has been given for the person under Part IACA of the *Crimes Act 1914*;
(d) a corresponding witness identity protection certificate has been given for the person under a corresponding witness identity protection law within the meaning of Part IACA of the *Crimes Act 1914*;
(e) the person is a participant as defined in the *Witness Protection Act 1994*;
(f) the person is or was on a witness protection program conducted by a State or Territory in which a complementary witness protection law (as defined in the *Witness Protection Act 1994*) is in force;
(g) the person is involved in administering such a program under such a law and the person has acquired an identity under that law.

***State or Territory privacy authority*** means a State or Territory authority (within the meaning of the *Privacy Act 1988*) that has functions to protect the privacy of individuals (whether or not the authority has other functions).

***this Act*** includes:

(a) the Accreditation Rules; and
(b) the Digital ID Data Standards; and
(c) the Digital ID Rules; and

(d) the service levels determined under section 76; and
(e) the Regulatory Powers Act as it applies in relation to this Act.

***verifiable credential*** means a tamper-evident credential with authorship that can be cryptographically verified.

## 10 Meaning of *attribute* of an individual

(1) An ***attribute*** of an individual means information that is associated with the individual, and includes information that is derived from another attribute.

(2) Without limiting subsection (1), an ***attribute*** of an individual includes the following:
(a) the individual's current or former name;
(b) the individual's current or former address;
(c) the individual's date of birth;
(d) information about whether the individual is alive or dead;
(e) the individual's phone number;
(f) the individual's email address;
(g) if the individual has a digital ID—the time and date the digital ID was created;
(h) biometric information of the individual;
(i) a restricted attribute of the individual;
(j) information or an opinion about the individual's:
(i) racial or ethnic origin; or
(ii) political opinions; or
(iii) membership of a political association; or
(iv) religious beliefs or affiliations; or
(v) philosophical beliefs; or
(vi) sexual orientation or practices.

Note 1: Accredited entities may collect, use or disclose attributes of an individual referred to in paragraphs (h) and (i) when providing accredited services only if their conditions of accreditation authorise this (see section 18).

Note 2: The collection, use and disclosure of attributes of an individual referred to in paragraph (j) by accredited entities when providing accredited services is prohibited (see section 41).

## 11 Meaning of *restricted attribute* of an individual

(1) A ***restricted attribute*** of an individual means:

(a) health information (within the meaning of the *Privacy Act 1988*) about the individual; or

(b) an identifier of the individual that has been issued or assigned by or on behalf of:

(i) the Commonwealth, a State or a Territory; or

(ii) an authority or agency of the Commonwealth, a State or a Territory; or

(iii) a government of a foreign country; or

(c) information or an opinion about the individual's criminal record; or

(d) information or an opinion about the individual's membership of a professional or trade association;

(e) information or an opinion about the individual's membership of a trade union;

(f) other information or opinion that is associated with an individual and is prescribed by the Accreditation Rules.

(2) Without limiting paragraph (1)(b), an identifier of an individual includes the following:

(a) the individual's tax file number (within the meaning of section 202A of the *Income Tax Assessment Act 1936*);

(b) the individual's medicare number (within the meaning of Part VII of the *National Health Act 1953*);

(c) the individual's healthcare identifier (within the meaning of the *Healthcare Identifiers Act 2010*);

(d) if the person holds a driver's licence issued under the law of a State or Territory—the number of that driver's licence.

## 12 Fit and proper person considerations

In having regard to whether an entity is a fit and proper person for the purposes of this Act, the Digital ID Regulator:

(a) must have regard to the matters (if any) specified in the Digital ID Rules; and

(b) may have regard to any other matters the Digital ID Regulator considers relevant.

# Chapter 2—Accreditation

## Part 1—Introduction

### 13 Simplified outline of this Chapter

# Part 2—Accreditation

## Division 1—Applying for accreditation

### 14 Application for accreditation

(1) An entity covered by subsection (2) may apply to the Digital ID Regulator for accreditation as one of the following kinds of accredited entities:

(a) an accredited attribute service provider;

(b) an accredited identity exchange provider;

(c) an accredited identity service provider;

(d) an entity that provides a service of a kind prescribed by the Accreditation Rules.

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

(2) An entity is covered by this section if the entity is one of the following:

(a) a body corporate incorporated by or under a law of the Commonwealth or a State or Territory;

(b) a registered foreign company within the meaning of the *Corporations Act 2001*;

(c) a Commonwealth entity, or a Commonwealth company, within the meaning of the *Public Governance, Performance and Accountability Act 2013*;

(d) a person or body that is an agency within the meaning of the *Freedom of Information Act 1982*;

(e) a body specified, or the person holding an office specified, in Part I of Schedule 2 to the *Freedom of Information Act 1982*;

(f) a department or authority of a State;

(g) a department or authority of a Territory.

## Division 2—Accreditation

### 15 Digital ID Regulator must decide whether to accredit an entity

(1) This section applies if an entity has made an application under section 14 for accreditation as an accredited entity.

(2) The Digital ID Regulator must decide:
  (a) to accredit the entity; or
  (b) to refuse to accredit the entity.

(3) The Digital ID Regulator must not accredit an entity:
  (a) as an accredited attribute service provider unless the entity is an attribute service provider; or
  (b) as an accredited identity exchange provider unless the entity is an identity exchange provider; or
  (c) as an accredited identity service provider unless the entity is an identity service provider; or
  (d) if Accreditation Rules made for the purposes of paragraph 14(1)(d) prescribe services—as an entity that provides services of the kind prescribed unless the entity provides services of that kind.

(4) The Digital ID Regulator must not accredit an entity if:
  (a) a direction under subsection 16(1) (about security) is in force in relation to the entity; or
  (b) if the Digital ID Regulator makes a requirement under paragraph 126(1)(a) in relation to the entity—the Digital ID Regulator is not satisfied that the entity has been assessed as being able to comply with this Act; or
  (c) Accreditation Rules made for the purposes of section 27 require specified criteria to be met and the entity does not meet the criteria; or
  (d) Accreditation Rules made for the purposes of section 27 require the Digital ID Regulator be satisfied of specified matters and the Digital ID Regulator is not satisfied of those matters.

(5) In deciding whether to accredit the entity, the Digital ID Regulator:

(a) must have regard to the matters (if any) prescribed by the Accreditation Rules; and

(b) may consult:

(i) the Information Commissioner; or

(ii) the Australian Securities and Investments Commission; or

(iii) the Australian Prudential Regulation Authority; or

(iv) the Australian Financial Complaints Authority; or

(v) the part of the Australian Signals Directorate known as the Australian Cyber Security Centre; or

(vi) any other body the Digital ID Regulator considers appropriate; and

(c) may have regard to the following:

(i) matters raised in consultations (if any) under paragraph (b);

(ii) matters relating to security (within the meaning of the *Australian Security Intelligence Organisation Act 1979*);

(iii) whether the entity is a fit and proper person;

(iv) any other matters the Digital ID Regulator considers relevant.

Note: In having regard to whether an entity is a fit and proper person for the purposes of subparagraph (c)(iii), the Digital ID Regulator must have regard to any matters specified in the Digital ID Rules and may have regard to any other matters considered relevant (see section 12).

(6) The Digital ID Regulator must:

(a) give written notice of a decision to accredit, or to refuse to accredit, the entity; and

(b) if the decision is to refuse to accredit the entity—give reasons for the decision to the entity.

(7) If the Digital ID Regulator decides to accredit the entity, the notice must also set out the following:

(a) the kind of accredited entity that the entity is accredited as;

(b) the day the accreditation comes into force;

(c) any conditions imposed on the entity's accreditation under subsection 18(2).

## 16 Minister's directions regarding accreditation

(1) The Minister may, in writing, direct the Digital ID Regulator to refuse to accredit an entity if, for reasons of security (within the meaning of the *Australian Security Intelligence Organisation Act 1979*), including on the basis of an adverse or qualified security assessment in respect of a person, the Minister considers it appropriate to do so.

(2) The Minister may, in writing, direct the Digital ID Regulator to suspend the accreditation of an accredited entity (either indefinitely or for a specified period) if, for reasons of security (within the meaning of the *Australian Security Intelligence Organisation Act 1979*), including on the basis of an adverse or qualified security assessment in respect of a person, the Minister considers it appropriate to do so.

(3) If the Minister gives a direction under subsection (1) or (2), the Digital ID Regulator must comply with the direction.

(4) The direction remains in force until revoked by the Minister. The Minister must notify the Digital ID Regulator and the entity if the Minister revokes the direction.

Note: The entity cannot be accredited again while the direction remains in force (see paragraph 15(4)(a)).

(5) A direction given under subsection (1) or (2) is not a legislative instrument.

## 17 Accreditation is subject to conditions

(1) The accreditation of an entity as an accredited entity is subject to the following conditions (the ***accreditation conditions***):

(a) the conditions set out in subsection 18(1);

(b) the conditions (if any) imposed by the Digital ID Regulator under subsection 18(2), including as varied under subsection 20(1);

(c) the conditions (if any) determined by the Accreditation Rules under subsection 18(6).

(2) An accredited entity must comply with the accreditation conditions that apply to the entity.

Note: Failure to comply with an accreditation condition may result in a suspension or revocation of the entity's accreditation (see sections 25 and 26).

## 18 Conditions on accreditation

*Conditions imposed by the Act*

(1) The accreditation of an entity as an accredited entity is subject to the condition that the accredited entity must comply with this Act.

*Conditions imposed by the Digital ID Regulator*

(2) The Digital ID Regulator may impose conditions on the accreditation of an entity, either at the time of accreditation or at a later time, if the Digital ID Regulator considers that doing so is appropriate in the circumstances.

(3) Conditions may be imposed under subsection (2) on application by the entity or on the Digital ID Regulator's own initiative.

(4) Without limiting subsection (2), a condition may be imposed for reasons of security (within the meaning of the *Australian Security Intelligence Organisation Act 1979*), including on the basis of an adverse or qualified security assessment in respect of a person.

(5) Without limiting subsection (2), the Digital ID Regulator may impose conditions relating to the following:

(a) any limitations, exclusions or restrictions in relation to the accredited services of the entity;

(b) the circumstances or manner in which the accredited services of the entity must be provided;

(c) the kinds of restricted attributes of individuals (if any) that the entity is authorised to collect or disclose and the circumstances in which such attributes may be collected or disclosed;

(d) the kinds of biometric information (if any) of an individual the entity is authorised to collect, use or disclose and the circumstances in which such information may be collected, used or disclosed;

(e) the entity's information technology systems through which the entity's accredited services are provided, including restrictions on changes to such systems;

(f) actions that the entity must take before the entity's accreditation is suspended or revoked.

*Conditions imposed by the Accreditation Rules*

(6) The Accreditation Rules may determine that the accreditation of each accredited entity, or each accredited entity included in a specified class, is subject to specified conditions.

(7) Without limiting subsection (6), the Accreditation Rules may impose conditions relating to the matters in subsection (5).

## 19 Requirements before Accreditation Rules impose conditions relating to restricted attributes or biometric information of individuals

(1) Subsection (2) applies if the Minister proposes to make Accreditation Rules for the purposes of subsection 18(6) providing that accredited entities, or specified kinds of accredited entities, are authorised to:

(a) collect or disclose restricted attributes of individuals; or

(b) collect, use or disclose biometric information of individuals.

Note: The Minister must also consult the Information Commissioner before making such rules (see paragraph 159(1)(b)).

(2) In deciding whether to make the rules, the Minister must have regard to the following matters:

(a) the potential harm that could result if the information were disclosed to an entity;
(b) community expectations about the collection, use or disclosure of the information;
(c) whether disclosure of the information is regulated by another law of the Commonwealth;
(d) any privacy impact assessment that has been conducted in relation to the proposal to make the rules;
(e) any other matter the Minister considers relevant.

## 20 Variation and revocation of conditions on accreditation

(1) The Digital ID Regulator may vary or revoke a condition imposed on an entity's accreditation under subsection 18(2):
(a) at any time, on the Digital ID Regulator's own initiative; or
(b) on application by the entity under section 21;
if the Digital ID Regulator considers it is appropriate to do so.

(2) Without limiting subsection (1), the Digital ID Regulator may have regard to the following matters when considering whether it is appropriate to vary or revoke a condition:
(a) matters relating to the security, reliability and stability of the Australian Government Digital ID System;
(b) matters relating to security (within the meaning of the *Australian Security Intelligence Organisation Act 1979*).

## 21 Applying for variation or revocation of conditions on accreditation

(1) An accredited entity may apply for a condition on the entity's accreditation to be varied or revoked.

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

(2) If, after receiving an application under subsection (1), the Digital ID Regulator refuses to vary or revoke a condition, the Digital ID Regulator must give to the entity written notice of the refusal, including reasons for the refusal.

## 22 Notice before changes to conditions on accreditation

(1) The Digital ID Regulator must not, on the Digital ID Regulator's own initiative:

(a) impose a condition under subsection 18(2) on an entity's accreditation after the entity has been accredited; or

(b) vary or revoke a condition under subsection 20(1);

unless the Digital ID Regulator has given the entity a written notice in accordance with subsection (2).

(2) The notice must:

(a) state the proposed condition, variation or revocation; and

(b) request the entity to give the Digital ID Regulator, within the period specified in the notice, a written statement relating to the proposed condition, variation or revocation.

(3) The Digital ID Regulator must consider any written statement given within the period specified in the notice before making a decision to:

(a) impose a condition under subsection 18(2) on an entity's accreditation; or

(b) vary or revoke a condition under subsection 20(1) on an entity's accreditation.

(4) This section does not apply if the Digital ID Regulator reasonably believes that the need to impose, vary or revoke the condition is serious and urgent.

(5) If this section does not apply to an entity because of subsection (4), the Digital ID Regulator must give a written statement of reasons to the entity as to why the Digital ID Regulator reasonably believes that the need to impose, vary or revoke the condition is serious and urgent.

(6) The statement of reasons must be given within 7 days after the condition is imposed, varied or revoked.

### 23 Notice of decision of changes to conditions on accreditation

(1) Subject to subsection (2), the Digital ID Regulator must give an entity written notice of a decision to impose, vary or revoke a condition on an entity's accreditation.

(2) The Digital ID Regulator is not required to give an entity notice of the decision if notice of the condition was given in a notice under subsection 15(7).

(3) The notice must:

(a) state the condition or the variation, or state that the condition is revoked; and

(b) state the day on which the condition, variation or revocation takes effect.

## Division 3—Varying, suspending and revoking accreditation

### 24 Varying accreditation

The Digital ID Regulator may vary the accreditation of an accredited entity to take account of a change in the accredited entity's name.

Note: The Digital ID Regulator can also vary conditions on accreditation (see section 20).

### 25 Suspension of accreditation

*Digital ID Regulator must suspend accreditation if Minister's direction is in force*

(1) The Digital ID Regulator must, in writing, suspend the accreditation of an accredited entity if a direction under subsection 16(2) is in force in relation to the entity.

*Digital ID Regulator may decide to suspend accreditation in other circumstances*

(2) The Digital ID Regulator may, in writing, suspend the accreditation of an accredited entity if:

(a) the Digital ID Regulator reasonably believes that the accredited entity has contravened or is contravening this Act; or

(b) the Digital ID Regulator reasonably believes that there has been a cyber security incident involving the entity; or

(c) the Digital ID Regulator reasonably believes that a cyber security incident involving the entity is imminent; or

(d) the Digital ID Regulator reasonably believes that, for reasons of security (within the meaning of the *Australian Security Intelligence Organisation Act 1979*), including on the basis of an adverse or qualified security assessment in respect of a person, it is appropriate to do so; or

(e) if the entity is a body corporate—the entity becomes a Chapter 5 body corporate (within the meaning of the *Corporations Act 2001*); or

(f) the Digital ID Regulator is satisfied that it is not appropriate for the entity to be an accredited entity; or

(g) circumstances specified in the Accreditation Rules apply in relation to the entity.

Note: The Digital ID Regulator may impose conditions on an entity's accreditation before suspending it (see paragraph 18(5)(f)) and can give directions to give effect to a decision to suspend an entity's accreditation (see paragraph 123(1)(e)).

(3) In determining whether the Digital ID Regulator is satisfied of the matter in paragraph (2)(f), regard may be had to whether the entity is a fit and proper person.

Note: In having regard to whether an entity is a fit and proper person, the Digital ID Regulator must have regard to any matters specified in the Digital ID Rules and may have regard to any other matters considered relevant (see section 12).

(4) Subsection (3) does not limit paragraph (2)(f).

*Digital ID Regulator may suspend accreditation on application*

(5) The Digital ID Regulator may, on application by an accredited entity, suspend the accreditation of the entity.

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

*Show cause notice must generally be given before decision to suspend*

(6) Before suspending the accreditation of an entity under subsection (2), the Digital ID Regulator must give a written notice (a ***show cause notice***) to the entity.

(7) The show cause notice must:

(a) state the grounds on which the Digital ID Regulator proposes to suspend the entity's accreditation; and

(b) invite the entity to give the Digital ID Regulator, within 28 days after the day the notice is given, a written statement

showing cause why the Digital ID Regulator should not suspend the accreditation.

*Exception—cyber security incident*

(8) Subsection (6) does not apply if the suspension is on a ground mentioned in paragraph (2)(b) or (c).

*Notice of suspension*

(9) If the Digital ID Regulator decides to suspend an entity's accreditation under subsection (2) or (5), the Digital ID Regulator must give the entity a written notice stating the following:

(a) that the entity's accreditation is suspended;

(b) if the entity is accredited as more than one kind of accredited entity—the accreditation that is suspended;

(c) the reasons for the suspension;

(d) the day the suspension is to start;

(e) if the accreditation is suspended for a period—the period of the suspension;

(f) if the accreditation is suspended until a specified event occurs or action is taken—the event or action;

(g) if the accreditation is suspended indefinitely—that fact.

*Effect of suspension*

(10) If an entity's accreditation is suspended under this section:

(a) the entity is taken not to be accredited while the suspension is in force; and

(b) if the entity holds an approval to participate in the Australian Government Digital ID System—the entity is taken not to hold the approval while the entity's accreditation is suspended.

*Revocation of suspension*

(11) If the accreditation of an entity is suspended under subsection (1), the suspension is revoked if the direction referred to in that subsection is revoked.

(12) If the Digital ID Regulator suspends an entity's accreditation under subsection (2), the Regulator may revoke the suspension by written notice to the entity.

(13) If the Digital ID Regulator suspends an entity's accreditation under subsection (5), the Regulator must revoke the suspension by written notice to the entity if the entity requests the suspension be revoked.

(14) A notice given under subsection (12) or (13) must specify the day the revocation takes effect.

## 26 Revocation of accreditation

*Revocation on Digital ID Regulator's own initiative*

(1) The Digital ID Regulator may, in writing, revoke an entity's accreditation if:

(a) the Digital ID Regulator reasonably believes that the accredited entity has contravened or is contravening this Act; or

(b) the Digital ID Regulator reasonably believes that there has been a cyber security incident involving the entity; or

(c) the Digital ID Regulator reasonably believes that a cyber security incident involving the entity is imminent; or

(d) the Digital ID Regulator reasonably believes that, for reasons of security (within the meaning of the *Australian Security Intelligence Organisation Act 1979*), including on the basis of an adverse or qualified security assessment in respect of a person, it is appropriate to do so; or

(e) if the entity is a body corporate—the entity becomes a Chapter 5 body corporate (within the meaning of the *Corporations Act 2001*); or

(f) the Digital ID Regulator is satisfied that it is not appropriate for the entity to be an accredited entity; or

(g) circumstances specified in the Accreditation Rules apply in relation to the entity.

Note: The Digital ID Regulator may impose conditions on an entity's accreditation before revoking it (see paragraph 18(5)(f)) and can give directions to give effect to a decision to revoke an entity's accreditation (see paragraph 123(1)(e)).

(2) In determining whether the Digital ID Regulator is satisfied of the matter in paragraph (1)(f), regard may be had to whether the entity is a fit and proper person.

Note: In having regard to whether an entity is a fit and proper person, the Digital ID Regulator must have regard to any matters specified in the Digital ID Rules and may have regard to any other matters considered relevant (see section 12).

(3) Subsection (2) does not limit paragraph (1)(f).

*Revocation on application*

(4) The Digital ID Regulator must, on application by an entity, revoke the entity's accreditation.

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

*Date of effect*

(5) The revocation takes effect on the day determined by the Digital ID Regulator.

*Approval must also be revoked*

(6) If:

(a) an entity's accreditation is revoked under subsection (1) or (4); and

(b) the entity holds an approval to participate in the Australian Government Digital ID System;

the Digital ID Regulator must at the same time revoke the entity's approval to participate.

*Show cause notice must generally be given before decision to revoke*

(7) Before revoking the accreditation of an entity under subsection (1), the Digital ID Regulator must give a written notice (a ***show cause notice***) to the entity.

(8) The show cause notice must:

(a) state the grounds on which the Digital ID Regulator proposes to revoke the entity's accreditation; and

(b) invite the entity to give the Digital ID Regulator, within 28 days after the day the notice is given, a written statement showing cause why the Digital ID Regulator should not revoke the accreditation.

*Exception—cyber security incident*

(9) Subsection (7) does not apply if the revocation is on a ground mentioned in paragraph (1)(b) or (c).

*Notice of revocation*

(10) If the Digital ID Regulator decides to revoke an entity's accreditation under subsection (1) or (4), the Digital ID Regulator must give the entity a written notice stating the following:

(a) that the entity's accreditation is to be revoked;

(b) if the entity is accredited as more than one kind of accredited entity—the accreditation that is to be revoked;

(c) the reasons for the revocation;

(d) the day the revocation is to take effect.

*Accreditation can be revoked even while suspended*

(11) Despite paragraph 25(10)(a), the Digital ID Regulator may revoke an entity's accreditation under this section even if a suspension is in force under section 25 in relation to the entity.

# Division 4—Accreditation Rules

## 27 Accreditation Rules

(1) The Accreditation Rules must provide for and in relation to matters concerning the accreditation of entities for the purposes of this Act.

(2) Without limiting subsection (1), the Accreditation Rules may deal with the following matters:

(a) requirements that entities must meet in order to become and remain an accredited entity, including requirements relating to the following:

(i) privacy;

(ii) security;

(iii) fraud control;

(iv) incident management and reporting;

(v) disaster recovery;

(vi) user experience and inclusion;

(b) without limiting paragraph (a), requirements relating to the conduct of, and reporting on, privacy impact assessments, fraud assessments and security assessments;

(c) technical, data or design standards relating to the provision of accredited services of accredited entities;

(d) without limiting paragraph (c), standards relating to the testing of the information technology systems of entities;

(e) the conduct of periodic reviews of an entity's compliance with specified requirements of the Accreditation Rules, including the timing of such reviews, who is to conduct such reviews and the provision of reports about such reviews to the Digital ID Regulator;

(f) the obligations of accredited entities in relation to monitoring their compliance with this Act;

(g) requirements relating to the collection, holding, use and disclosure of personal information of individuals;

(h) matters relating to representatives or nominees of individuals in relation to the creation, maintenance or deactivation of digital IDs of individuals;

(i) requirements or restrictions relating to the generation of digital IDs for children.

Note: In relation to subparagraph (2)(a)(iv), the Digital ID Rules may also provide for such arrangements in relation to incidents that occur within the Australian Government Digital ID System (see subsection 74(1)).

# Division 5—Other matters relating to accredited entities

## 28 Digital IDs must be deactivated on request

(1) This section applies if an accredited identity service provider generates a digital ID of an individual.

(2) The accredited identity service provider must, if requested to do so by the individual, deactivate the digital ID of the individual as soon as practicable after receiving the request.

## 29 Accredited services must be accessible and inclusive

(1) The Accreditation Rules must provide for and in relation to requirements relating to the accessibility and useability of the accredited services of accredited entities.

(2) Without limiting subsection (1), the Accreditation Rules may deal with the following matters:

(a) requirements to comply with accessibility standards or guidelines;

(b) requirements relating to useability testing;

(c) requirements relating to device or browser access.

# Chapter 3—Privacy

## Part 1—Introduction

### 30 Simplified outline of this Chapter

### 31 Chapter applies to accredited entities only to the extent the entity is providing accredited services etc.

This Chapter applies to an accredited entity only to the extent the entity is:

(a) providing its accredited services; or

(b) doing things that are incidental or ancillary to the provision of those services.

### 32 APP-equivalent agreements

The Minister may, on behalf of the Commonwealth, enter into an agreement (an ***APP-equivalent agreement***) with an entity that prohibits the entity from collecting, holding, using or disclosing personal information in any way that would, if the entity were an organisation within the meaning of the *Privacy Act 1988*, breach an Australian Privacy Principle.

# Part 2—Privacy

## Division 1—Interaction with the Privacy Act 1988

### 33 Extended meaning of *personal information* in relation to accredited entities

To the extent not already covered by the definition of ***personal information*** within the *Privacy Act 1988*, attributes of individuals, to the extent that they are in the possession or control of accredited entities, are taken, for the purposes of that Act, to be personal information about an individual.

Note 1: This section has the effect of extending the meaning of personal information in the *Privacy Act 1988* as it applies to accredited entities to mirror the meaning of that term as it is used in this Act (see section 9).

Note 2: This means that the requirements in the *Privacy Act 1988* about collecting, using and disclosing personal information under that Act extend to attributes of individuals to the extent that information is in the possession or control of accredited entities. However, this applies only to the extent the information is collected, used or disclosed when those entities are providing their accredited services (see section 31).

### 34 Privacy obligations for non-APP entities

(1) This section applies to an accredited entity that is not an APP entity.

Note: The obligations of accredited entities that are APP entities in relation to the handling of personal information are set out in the *Privacy Act 1988*.

(2) The accredited entity must not do an act or engage in a practice with respect to personal information unless:

(a) the *Privacy Act 1988* applies in relation to the act or practice as if the entity were an organisation within the meaning of that Act; or

(b) a law of a State or Territory that provides for all of the following applies in relation to the act or practice:

(i) protection of personal information comparable to that provided by the Australian Privacy Principles;

(ii) monitoring of compliance with the law;

(iii) a means for an individual to seek recourse if the individual's personal information is dealt with in a way contrary to the law; or

(c) all of the following apply:

(i) neither paragraph (a) nor (b) apply to the acts or practices of the entity;

(ii) the entity has an APP-equivalent agreement with the Commonwealth;

(iii) the agreement includes a term that prohibits the entity from collecting, holding, using or disclosing personal information in any way that would, if the entity were an organisation within the meaning of the *Privacy Act 1988*, breach an Australian Privacy Principle.

### 35 Contraventions of privacy obligations in APP-equivalent agreements

(1) This section applies to an entity if the entity has an APP-equivalent agreement with the Commonwealth.

(2) An act or practice of the entity that contravenes a term of the agreement in relation to an individual and collecting, holding, using or disclosing their personal information is taken to be:

(a) an interference with the privacy of the individual for the purposes of the *Privacy Act 1988*; and

(b) covered by sections 13 and 13G of that Act.

Note: An act or practice that is, or may be, an interference with privacy may be the subject of a complaint under section 36 of the *Privacy Act 1988*.

(3) The entity is taken, for the purposes of Part V of the *Privacy Act 1988* and any other provision of that Act that relates to that Part, to be an organisation (within the meaning of that Act) if:

(a) an act or practice of the entity has contravened, or may have contravened, the term of the agreement in relation to an individual; and

(b) the act or practice is the subject of a complaint to, or an investigation by, the Information Commissioner under Part V of the *Privacy Act 1988*.

(4) Sections 80V and 80W of the *Privacy Act 1988* apply in relation to the term of the agreement as if the term were a provision of that Act.

## 36 Contraventions of Division 2 are interferences with privacy

(1) An act or practice of an accredited entity that contravenes a provision of Division 2 of this Part in relation to personal information about an individual is taken to be:

(a) an interference with the privacy of the individual for the purposes of the *Privacy Act 1988*; and

(b) covered by sections 13 and 13G of that Act.

Note: An act or practice that is, or may be, an interference with privacy may be the subject of a complaint under section 36 of the *Privacy Act 1988*.

(2) The respondent to a complaint under the *Privacy Act 1988* about the act or practice, other than an act or practice of an agency or organisation, is the entity that engaged in the act or practice.

(3) The entity is taken, for the purposes of Part V of the *Privacy Act 1988* and any other provision of that Act that relates to that Part, to be an organisation if:

(a) the act or practice of the entity that contravenes a provision of Division 2 of this Part is the subject of a complaint to, or an investigation by, the Information Commissioner under Part V of the *Privacy Act 1988*; and

(b) the entity is not an agency or organisation.

(4) In this section:

***agency*** has the same meaning as in the *Privacy Act 1988*.

***organisation*** has the same meaning as in the *Privacy Act 1988*.

### 37 Notification of eligible data breaches—accredited entities that are APP entities

(1) This section applies to an accredited entity if the entity:

(a) is an APP entity; and

(b) is aware that there are reasonable grounds to believe that there has been an eligible data breach (within the meaning of the *Privacy Act 1988*) of the entity relating to the entity's accredited services; and

(c) is required under section 26WK of the *Privacy Act 1988* to give the Information Commissioner a statement that complies with subsection 26WK(3) of that Act.

(2) The entity must also give a copy of the statement to the Digital ID Regulator at the same time as the statement is given to the Information Commissioner.

### 38 Notification of eligible data breaches—accredited entities that are not APP entities

(1) This section applies to an accredited entity that is not an APP entity.

(2) Despite subsection (1), this section does not apply to an accredited entity if:

(a) the entity is a department or authority of a State or Territory; and

(b) a law of the State or Territory provides for a scheme for the notification of data breaches that:

(i) covers the entity; and

(ii) is comparable to the scheme provided for in Part IIIC of the *Privacy Act 1988*.

Note: See section 39 for requirements in relation to these entities.

(3) Part IIIC of the *Privacy Act 1988*, and any other provision of that Act that relates to that Part, apply in relation to the accredited entity as if the entity were an APP entity.

(4) If:

(a) the accredited entity is aware that there are reasonable grounds to believe that there has been an eligible data breach (within the meaning of the *Privacy Act 1988*) of the entity relating to the entity's accredited services; and

(b) because of the operation of subsection (3), the entity is required under section 26WK of that Act to give the Information Commissioner a statement that complies with subsection 26WK(3) of that Act;

the entity must also give a copy of the statement to the Digital ID Regulator at the same time as the statement is given to the Information Commissioner.

## 39 Notification of corresponding data breaches—accredited State or Territory entities that are not APP entities

(1) This section applies to an accredited entity if:

(a) the entity is not an APP entity; and

(b) the entity is a department or authority of a State or Territory; and

(c) the entity is required under a law of the State or Territory to give a statement (however described) that corresponds to section 26WK of the *Privacy Act 1988* to another entity (the ***notified entity***); and

(d) the statement relates to the accredited services of the entity.

(2) The entity must also give a copy of the statement to the Digital ID Regulator and the Information Commissioner at the same time as the statement is given to the notified entity.

## 40 Additional function of the Information Commissioner

In addition to the Information Commissioner's functions under the *Privacy Act 1988*, the Information Commissioner has the function

of providing advice, on request by the Digital ID Regulator, on matters relating to the operation of this Act.

# Division 2—Additional privacy safeguards

## 41 Collection etc. of certain attributes of individuals is prohibited

An accredited entity must not intentionally collect, use or disclose the following attributes of an individual:

(a) information or an opinion about an individual's racial or ethnic origin;

(b) information or an opinion about an individual's political opinions;

(c) information or an opinion about an individual's membership of a political association;

(d) information or an opinion about an individual's religious beliefs or affiliations;

(e) information or an opinion about an individual's philosophical beliefs;

(f) information or an opinion about an individual's sexual orientation or practices.

Civil penalty: 300 penalty units.

## 42 Individuals must expressly consent to disclosure of certain attributes of individuals to relying parties

When verifying the identity of an individual or authenticating the digital ID of, or information about, an individual to a relying party, an accredited entity must not disclose any of the following attributes of the individual to the relying party without the express consent of the individual:

(a) the individual's name;

(b) the individual's address;

(c) the individual's date of birth;

(d) the individual's phone number;

(e) the individual's email address;

(f) an attribute of a kind prescribed by the Accreditation Rules.

Civil penalty: 300 penalty units.

### 43 Disclosure of restricted attributes of individuals

(1) When verifying the identity of an individual or authenticating the digital ID of, or information about, an individual to a relying party, an accredited entity must not disclose a restricted attribute of the individual to the relying party without the express consent of the individual.

Civil penalty: 300 penalty units.

(2) An accredited entity must not disclose a restricted attribute of an individual to a relying party that is not a participating relying party if the accredited entity's conditions on accreditation do not include an authorisation to disclose the restricted attribute to the relying party.

Civil penalty: 300 penalty units.

(3) A participating relying party must not, while participating in the Australian Government Digital ID System, collect a restricted attribute of an individual if the relying party's approval to participate in the system does not include a condition that authorises the relying party to collect the restricted attribute.

Civil penalty: 300 penalty units.

### 44 Restricting the disclosure of unique identifiers

(1) This section applies if:

(a) an accredited entity (the ***assigning entity***) assigns a unique identifier to an individual within a digital ID system; and

(b) the assigning entity discloses the unique identifier to another accredited entity or to a relying party.

(2) The assigning entity must not disclose the unique identifier to any other entity other than:

(a) if the unique identifier was disclosed to another accredited entity—the other accredited entity; or

(b) if the unique identifier was disclosed to a relying party—the relying party.

Civil penalty: 300 penalty units.

(3) The accredited entity or relying party to whom the unique identifier is disclosed must not disclose the unique identifier to any other entity.

Civil penalty: 300 penalty units.

(4) Subsections (2) and (3) do not apply if the disclosure of the unique identifier is for one or more of the following purposes:

(a) detecting, reporting or investigating a contravention, or an alleged contravention, of a provision of this Act;

(b) conducting proceedings in relation to a contravention, or an alleged contravention, of a civil penalty provision of this Act;

(c) detecting, reporting or investigating either of the following within a digital ID system:

(i) a digital ID fraud incident;

(ii) a cyber security incident:

(d) conducting an assessment of the matter referred to in paragraph 33C(1)(g) of the *Privacy Act 1988* (about assessments by the Information Commissioner in relation to the handling and maintenance of personal information in accordance with certain aspects of this Act);

(e) detecting, reporting, investigating or prosecuting an offence against a law of the Commonwealth, a State or a Territory.

Note: A person who wishes to rely on this subsection bears an evidential burden in relation to the matter mentioned in this subsection (see section 96 of the Regulatory Powers Act).

(5) Subsections (2) and (3) also do not apply if the unique identifier is disclosed to another entity if the other entity is facilitating access to the entity for whom the unique identifier was created.

Note: A person who wishes to rely on this subsection bears an evidential burden in relation to the matter mentioned in this subsection (see section 96 of the Regulatory Powers Act).

### 45 Restrictions on collecting, using and disclosing biometric information

(1) An accredited entity may collect, use or disclose biometric information of an individual only if:

(a) the collection, use or disclosure is authorised under section 46 or 47; and

(b) unless the collection, use or disclosure is authorised under paragraph 46(3)(a) or subsection 46(5), (6) or (8)—the individual to whom the information relates has expressly consented to the collection, use or disclosure of the biometric information.

Civil penalty: 300 penalty units.

(2) To avoid doubt, and without limiting subsection (1), an accredited entity must not:

(a) collect, use or disclose biometric information of an individual for the purpose of one-to-many matching of the individual; or

(b) collect, use or disclose biometric information of an individual to determine whether the individual has multiple digital IDs.

(3) ***One-to-many matching*** means the process of comparing a kind of biometric information of an individual against that kind of biometric information of individuals generally to identify the particular individual.

### 46 Authorised collection, use and disclosure of biometric information of individuals—general rules

(1) An accredited entity is authorised to collect, use or disclose biometric information of an individual if:

(a) the entity is an accredited identity service provider; and

(b) the entity's conditions on accreditation authorise the collection, use or disclosure of the biometric information; and

(c) the biometric information of the individual is collected, used or disclosed for the purposes of the accredited entity doing either or both of the following:

(i) verifying the identity of the individual;

(ii) authenticating the individual to their digital ID.

(2) An accredited entity is authorised to collect, use or disclose biometric information of an individual if:

(a) the biometric information is contained in a verifiable credential that is in control of the individual; and

(b) the collection, use or disclosure complies with any requirements prescribed by the Accreditation Rules.

(3) An accredited entity is authorised to disclose biometric information of an individual to a law enforcement agency (within the meaning of the *Australian Crime Commission Act 2002*) only if:

(a) the information is disclosed under a warrant issued by a magistrate, judge or member of a tribunal; or

(b) the information is disclosed with the consent of the individual to whom the biometric information relates, or purports to relate, and the disclosure is for the purpose of:

(i) verifying the identity of the individual; or

(ii) investigating or prosecuting an offence against a law of the Commonwealth, a State or a Territory.

(4) Subsection (3) applies despite any law of the Commonwealth, a State or a Territory (whether enacted or made before or after this subsection) or a warrant, authorisation or order issued under such a law.

(5) An accredited entity is authorised to disclose biometric information of an individual if the disclosure is to the individual to whom the biometric information relates.

(6) An accredited entity is authorised to retain, use or disclose biometric information of an individual if:

(a) the entity is an accredited identity service provider; and

(b) the entity collected the information in accordance with subsection (1); and

(c) the information is retained, used or disclosed for the purposes of undertaking testing in relation to the information; and

(d) the entity complies with any requirements prescribed by the Accreditation Rules.

(7) Without limiting paragraph (6)(d), Accreditation Rules made for the purposes of that paragraph may prescribe requirements in relation to the following matters:

(a) the purposes for which testing may be undertaken;

(b) the kinds of testing that may be undertaken using biometric information;

(c) the circumstances in which testing of the biometric information may be undertaken;

(d) the manner in which the biometric information that has been retained for testing must be destroyed;

(e) the preparation, content, approval and implementation of ethics plans relating to the testing of the biometric information;

(f) obtaining express consent of individuals to whom the biometric information relates;

(g) reporting of testing results to the Digital ID Regulator.

(8) An accredited entity is authorised to retain, use or disclose biometric information of an individual if:

(a) the entity is an accredited identity service provider; and

(b) the entity collected the information in accordance with subsection (1); and

(c) the information is retained, used or disclosed for the purposes of preventing or investigating a digital ID fraud incident; and

(d) the entity complies with any requirements prescribed by the Accreditation Rules.

(9) Without limiting paragraph (8)(d), Accreditation Rules made for the purposes of that paragraph may prescribe requirements in relation to the following matters:

(a) the manner in which biometric information that has been retained for preventing or investigating digital ID fraud incidents must be destroyed;

(b) the reporting of fraud prevention or investigation activities to the Digital ID Regulator.

## 47 Accredited identity service providers may collect etc. biometric information for purposes of government identity documents

(1) This section applies if:

(a) an accredited entity collects biometric information of an individual under subparagraph 46(1)(c)(i) for the purpose of verifying the identity of the individual; and

(b) the accredited entity has verified that the biometric information is legitimate.

Note: Because this Chapter applies to an entity only to the extent that the entity is providing accredited services or doing things that are incidental or ancillary to the provision of those services (see section 31), this section does not affect information collected, retained, etc. by the entity in any other capacity.

(2) If the entity is covered by subsection (3), the entity may collect, use, disclose or retain the biometric information for the purposes of issuing a document or other credential that:

(a) contains personal information about the individual; and

(b) the individual has consented to the issue of; and

(c) can be used to assist the individual to prove the individual's age or identity or a permission or authorisation that the individual holds; and

(d) is issued by or on behalf of the entity.

(3) The entities covered by this subsection are as follows:

(a) a body corporate incorporated by or under a law of the Commonwealth or a State or Territory;

(b) a Commonwealth entity, or a Commonwealth company, within the meaning of the *Public Governance, Performance and Accountability Act 2013*; or

(c) a person or body that is an agency within the meaning of the *Freedom of Information Act 1982*;

(d) a body specified, or the person holding an office specified, in Part I of Schedule 2 to the *Freedom of Information Act 1982*;

(e) a department or authority of a State;

(f) a department or authority of a Territory.

(4) Subsection (2) applies despite anything else in this Division.

(5) If:

(a) the entity (the ***first entity***) is not covered by subsection (3); and

(b) the first entity has a written agreement with another entity (the ***government entity***) that is covered by that subsection; and

(c) the agreement provides for the first entity to disclose the biometric information of the individual to the government entity for the purposes of issuing a document or other credential that:

(i) contains personal information about the individual; and

(ii) the individual has consented to the issue of; and

(iii) can be used to assist the individual to prove the individual's age or identity or a permission or authorisation that the individual holds; and

(iv) is issued by or on behalf of the entity;

the entity may disclose the biometric information in accordance with the agreement if the disclosure occurs within 14 days after the biometric information is collected.

## 48 Destruction of biometric information of individuals

(1) Subject to subsections (3) and (4), if an accredited identity service provider collects biometric information of an individual for the purposes of verifying an individual's identity, the provider must destroy the information immediately after the verification is complete.

Civil penalty: 300 penalty units.

(2) Subject to subsections (3) and (4), if:

(a) an accredited entity collects biometric information of an individual with the express consent of the individual to whom the information relates; and

(b) the information is collected for the purposes of authenticating the individual to their digital ID; and

(c) the individual withdraws their consent;

the provider must destroy the information immediately after the consent is withdrawn.

(3) If an accredited entity retains biometric information of an individual in accordance with subsection 46(6) (about testing), the entity must destroy the information at the earlier of:

(a) the completion of testing the information; and

(b) 14 days after the entity collects the information.

Civil penalty: 300 penalty units.

(4) If an accredited entity retains biometric information of an individual in accordance with subsection 46(8) (about preventing investigating digital ID fraud incidents), the entity must destroy the information at the earlier of:

(a) immediately after the completion of activities relating to the prevention or investigation of the digital ID fraud incident (as the case may be); and

(b) 14 days after the entity collects the information.

Civil penalty: 300 penalty units.

## 49 Other rules relating to biometric information

(1) The Accreditation Rules may provide for and in relation to the collection, use, disclosure, storage or destruction of biometric information of individuals by accredited entities.

(2) Without limiting subsection (1), the Accreditation Rules may provide for requirements relating to quality, security or fraud.

## 50 Data profiling to track online behaviour is prohibited

(1) An accredited entity must not use or disclose information if:

(a) the information is personal information about an individual that is in the entity's possession or control; and

(b) the information is any of the following:

(i) information about the services provided by the entity that the individual has accessed, or attempted to access;

(ii) information relating to how or when access was obtained or attempted to be obtained by the individual;

(iii) information relating to the method of access or attempted access by the individual;

(iv) the date and time the individual's identity was verified.

Civil penalty: 300 penalty units.

(2) Subsection (1) applies even if the individual has consented to the use or disclosure.

(3) However, subsection (1) does not apply if the use or disclosure:

(a) is for purposes relating to the provision the entity's accredited services (including improving the performance or useability of the entity's information technology systems through which those services are provided); or

(b) is for the purposes of the entity complying with this Act; or

(c) is required or authorised by or under a law of the Commonwealth, a State or a Territory.

Note: A person who wishes to rely on this subsection bears an evidential burden in relation to the matter mentioned in this subsection (see section 96 of the Regulatory Powers Act).

## 51 Personal information must not be used or disclosed for prohibited enforcement purposes

(1) An accredited entity must not use or disclose personal information that is in the entity's possession or control for the purposes of enforcement related activities conducted by, or on behalf of, an enforcement body unless:

(a) at the time the information is used or disclosed, the accredited entity is satisfied that the enforcement body reasonably suspects that a person has committed an offence against a law of the Commonwealth, a State or a Territory, or started proceedings against a person for such an offence; or

(b) at the time the information is used or disclosed, the accredited entity is satisfied that the enforcement body reasonably suspects that a person has breached a law imposing a penalty or sanction, or has started proceedings against a person in relation to the breach; or

(c) the information is used or disclosed under a warrant issued by a magistrate, judge or member of a tribunal; or

(d) the information is used or disclosed for the purposes of reporting a suspected or actual digital ID fraud incident or suspected or actual cyber security incident; or

(e) the information is used or disclosed by the accredited entity for the purposes of complying with this Act.

Civil penalty: 300 penalty units.

(2) Despite section 96 of the Regulatory Powers Act, in proceedings for a civil penalty order against a person for a contravention of subsection (1), the person does not bear an evidential burden in relation to the matter in paragraphs (1)(a) to (e).

(3) This section applies despite:

(a) section 86E of the *Crimes Act 1914* (about disclosure of personal information to certain entities for integrity purposes); and

(b) any other law of the Commonwealth, a State or a Territory, whether enacted or made before or after the commencement of this section.

## 52 Personal information must not be used or disclosed for prohibited marketing purposes

(1) An accredited entity must not use or disclose personal information about an individual that is in the entity's possession or control for any of the following purposes:

(a) offering to supply goods or services;

(b) advertising or promoting goods or services;

(c) enabling another entity to offer to supply goods or services;

(d) enabling another entity to advertise or promote goods or services;

(e) market research.

Civil penalty: 300 penalty units.

(2) Subsection (1) does not apply to the disclosure of personal information about an individual if:

(a) the information is disclosed to an individual for the purposes of:

(i) offering to supply the entity's accredited services; or

(ii) advertising or promoting the entity's accredited services; and

(b) the information is disclosed to the individual with the individual's express consent.

Note: A person who wishes to rely on this subsection bears an evidential burden in relation to the matter mentioned in this subsection (see section 96 of the Regulatory Powers Act).

## 53 Accredited identity exchange providers must not retain certain attributes of individuals

(1) This section applies if, during an authenticated session, an accredited identity exchange provider receives any of the following attributes of an individual:

(a) a restricted attribute of the individual;

(b) the individual's name;

(c) the individual's address;

(d) the individual's date of birth;
(e) the individual's phone number;
(f) the individual's email address;
(g) an attribute of a kind prescribed by the Accreditation Rules.

(2) The accredited identity exchange provider must not retain the attribute of the individual after the end of the authenticated session.

Civil penalty: 300 penalty units.

(3) In this section:

***authenticated session*** has the meaning given by the Accreditation Rules.

# Chapter 4—The Australian Government Digital ID System

## Part 1—Introduction

### 54 Simplified outline of this Chapter

# Part 2—The Australian Government Digital ID System

## Division 1—The Australian Government Digital ID System

### 55 Digital ID Regulator must oversee and maintain the Australian Government Digital ID System

(1) The Digital ID Regulator must oversee and maintain a digital ID system.

(2) The ***Australian Government Digital ID System*** means the digital ID system overseen and maintained by the Digital ID Regulator under subsection (1).

### 56 Circumstances in which entities may provide or receive services within the Australian Government Digital ID System

(1) An entity mentioned in column 1 of an item in the following table may provide or receive services within the Australian Government Digital ID System if the entity satisfies the requirements set out in column 2 of that item.

**Services provided or received within the Australian Government Digital ID System**

| Item | Column 1<br>Entity | Column 2<br>Requirements |
|---|---|---|
| 1 | Attribute service provider | (a) the attribute service provider:<br>(i) must be an accredited attribute service provider; and<br>(ii) must hold an approval under section 59 to participate in the system; and<br>(b) the participation start day for the |

| **Services provided or received within the Australian Government Digital ID System** | | |
|---|---|---|
| **Item** | **Column 1**<br>**Entity** | **Column 2**<br>**Requirements** |
| | | attribute service provider must have arrived or passed |
| 2 | Identity exchange provider | (a) the identity exchange provider:<br>(i) must be an accredited identity exchange provider; and<br>(ii) must hold an approval under section 59 to participate in the system; and<br>(b) the participation start day for the identity exchange provider must have arrived or passed |
| 3 | Identity service provider | (a) the identity service provider:<br>(i) must be an accredited identity service provider; and<br>(ii) must hold an approval under section 59 to participate in the system; and<br>(b) the participation start day for the identity service provider must have arrived or passed |
| 4 | Relying party | (a) the relying party:<br>(i) must be an Australian entity or registered foreign company (within the meaning of the *Corporations Act 2001*); and<br>(ii) must hold an approval under section 59 to participate in the system; and |

| **Services provided or received within the Australian Government Digital ID System** | | |
|---|---|---|
| **Item** | **Column 1**<br>**Entity** | **Column 2**<br>**Requirements** |
| | | (b) the participation start day for the relying party must have arrived or passed |
| 5 | An entity that provides services of a kind prescribed by the Accreditation Rules for the purposes of paragraph 14(1)(d) | (a) the entity:<br>(i) must be accredited to provide services of that kind; and<br>(ii) must hold an approval under section 59 to participate in the system; and<br>(iii) must meet any other requirements prescribed by the Digital ID Rules; and<br>(b) the participation start day for the entity must have arrived or passed |

(2) An entity contravenes this subsection if:

(a) the entity provides or receives services within the Australian Government Digital ID System; and

(b) the entity is not an entity mentioned in column 1 of an item in the table in subsection (1).

Civil penalty: 200 penalty units.

(3) An entity contravenes this subsection if:

(a) the entity provides or receives services within the Australian Government Digital ID System; and

(b) the entity is an entity mentioned in column 1 of an item in the table in subsection (1); and

(c) the entity does not satisfy one or more requirements set out in column 2 of that item.

Civil penalty: 200 penalty units.

## Division 2—Participating in the Australian Government Digital ID System

### 57 Phasing-in of participation in the Australian Government Digital ID System

(1) The Minister may, by legislative instrument, determine the entities that may apply to the Digital ID Regulator for approval to participate in the Australian Government Digital ID System.

Note: The determination may specify entities by class (see subsection 33(3A) of the *Acts Interpretation Act 1901*).

(2) The determination may specify entities in any way, including by reference to:

(a) whether the entities are relying parties or accredited entities; or

(b) kinds of relying parties; or

(c) kinds of accredited entities; or

(d) whether the entity belongs to the public or private sector.

(3) The Minister:

(a) must not revoke the determination; and

(b) may vary the determination only to specify additional kinds of entities that may apply.

### 58 Applying for approval to participate in the Australian Government Digital ID System

(1) An entity may apply to the Digital ID Regulator for approval to participate in the Australian Government Digital ID System if:

(a) the entity is covered by subsection (2); and

(b) the entity is:

(i) an accredited entity; or

(ii) an entity that has applied for accreditation under section 14; or

(iii) a relying party that is an Australian entity; or

(iv) a relying party that is a registered foreign company (within the meaning of the *Corporations Act 2001*).

Note 1: Only entities of particular kinds can be, or apply to be, an accredited entity (see subsection 14(2)).

Note 2: See Part 5 of Chapter 8 for matters relating to applications.

(2) An entity is covered by this subsection if:

(a) the entity is:

(i) a Commonwealth entity, or a Commonwealth company, within the meaning of the *Public Governance, Performance and Accountability Act 2013*; or

(ii) a person or body that is an agency within the meaning of the *Freedom of Information Act 1982*; or

(iii) a body specified, or the person holding an office specified, in Part I of Schedule 2 to the *Freedom of Information Act 1982*; or

(b) the entity is covered by a determination made under section 57.

## 59 Approval to participate in the Australian Government Digital ID System

(1) The Digital ID Regulator may approve an entity to participate in the Australian Government Digital ID System if:

(a) the entity has made an application under section 58; and

(b) unless the entity is a relying party—the entity is an accredited entity; and

(c) the Digital ID Regulator is satisfied that the entity will comply with the Digital ID Data Standards that apply in relation to the entity; and

(d) if the Digital ID Regulator makes a requirement under paragraph 126(1)(a) in relation to the entity—the entity has been assessed as being able to comply with this Act; and

(e) the Digital ID Regulator is satisfied that it is appropriate to approve the entity to participate in the system; and

(f) any other requirements prescribed by the Digital ID Rules are met.

(2) Without limiting paragraph (1)(e), the Digital ID Regulator may have regard to the following matters when considering whether it is appropriate to approve the entity:

(a) matters relating to security (within the meaning of the *Australian Security Intelligence Organisation Act 1979*);

(b) whether the entity is a fit and proper person;

(c) whether the entity has appropriate procedures for dealing with the identities (whether real or not, and whether assumed or not) of shielded persons.

Note: In having regard to whether an entity is a fit and proper person for the purposes of paragraph (b), the Digital ID Regulator must have regard to any matters specified in the Digital ID Rules and may have regard to any other matters considered relevant (see section 12).

(3) Without limiting paragraph (1)(f), the Digital ID Rules may prescribe requirements relating to the security, reliability and stability of the Australian Government Digital ID System.

(4) However, the Digital ID Regulator must not approve an entity to participate in the Australian Government Digital ID System if a direction under subsection 60(1) is in force in relation to the entity.

(5) The Digital ID Regulator must:

(a) give written notice of a decision to approve, or to refuse to approve, an entity to participate in the Australian Government Digital ID System; and

(b) if the decision is to refuse to approve the entity—give reasons for the decision to the entity.

(6) If the Digital ID Regulator approves an entity to participate in the Australian Government Digital ID System, the notice must set out:

(a) the day the approval comes into force; and

(b) any conditions imposed on the approval under subsection 62(2); and

(c) the day on which the entity must begin to participate in the Australian Government Digital ID System.

Note: It is a condition of the entity's approval that the entity begin to participate on the day referred to in paragraph (c) (see paragraph

62(1)(c)). An entity must not begin to participate before that day (see the requirements in column 2 of the table in subsection 56(1)).

## 60 Minister's directions regarding participation

(1) The Minister may, in writing, direct the Digital ID Regulator to refuse to approve the entity to participate in the digital ID system under section 59 if, for reasons of security (within the meaning of the *Australian Security Intelligence Organisation Act 1979*), including on the basis of an adverse or qualified security assessment in respect of a person, the Minister considers it appropriate to do so.

(2) The Minister may, in writing, direct the Digital ID Regulator to suspend the approval of an entity to participate in the digital ID system under subsection 69(1) (either indefinitely or for a specified period) if, for reasons of security (within the meaning of the *Australian Security Intelligence Organisation Act 1979*), including on the basis of an adverse or qualified security assessment in respect of a person, the Minister considers it appropriate to do so.

(3) If the Minister gives a direction under subsection (1) or (2), the Digital ID Regulator must comply with the direction.

(4) The direction remains in force until revoked by the Minister. The Minister must notify the Digital ID Regulator and the entity if the Minister revokes the direction.

Note: The entity cannot begin to participate again while the direction remains in force (see subsection 59(4)).

(5) A direction given under subsection (1) or (2) is not a legislative instrument.

## 61 Approval to participate in the Australian Government Digital ID System is subject to conditions

(1) The approval of an entity to participate in the Australian Government Digital ID System is subject to the following conditions (the ***approval conditions***):

(a) the conditions set out in subsection 62(1);

(b) the conditions (if any) imposed by the Digital ID Regulator under subsection 62(2), including as varied under subsection 64(1);

(c) the conditions (if any) determined by the Digital ID Rules for the purposes of subsection 62(6).

(2) An entity that holds an approval to participate in the Australian Government Digital ID System must comply with the approval conditions that apply to the entity.

Note: Failure to comply with an approval condition may result in a suspension or revocation of the entity's approval to participate (see sections 69 and 70).

## 62 Conditions on approval to participate in the Australian Government Digital ID System

*Conditions imposed by the Act*

(1) The approval of an entity to participate in the Australian Government Digital ID System is subject to the following conditions:

(a) unless the entity is a relying party—the entity must be an accredited entity;

(b) if the entity is an accredited entity:

(i) the entity must participate in the Australian Government Digital ID System only as the kind of accredited entity it is accredited as; and

(ii) the entity must provide only its accredited services in the Australian Government Digital ID System;

(c) the entity must begin to participate in the Australian Government Digital ID System on the entity's participation start day;

(d) the entity must comply with this Act.

*Conditions imposed by the Digital ID Regulator*

(2) The Digital ID Regulator may impose conditions on the approval of an entity to participate in the Australian Government Digital ID

System, either at the time of approval or at a later time, if the Digital ID Regulator considers that doing so is appropriate in the circumstances.

(3) Conditions may be imposed under subsection (2) on application by the entity or on the Digital ID Regulator's own initiative.

(4) Without limiting subsection (2), a condition may be imposed for reasons of security (within the meaning of the *Australian Security Intelligence Organisation Act 1979*), including on the basis of an adverse or qualified security assessment in respect of a person.

(5) Without limiting subsection (2), the Digital ID Regulator may impose conditions that relate to any of the following:

(a) the kind of accredited entity or participating relying party that the entity must directly connect to in order to participate in the Australian Government Digital ID System;

(b) the kinds of attributes of individuals that the entity is authorised to collect or disclose and the circumstances in which such attributes may be collected or disclosed;

(c) for an accredited entity—the circumstances in which the entity may or must not provide its accredited services within the Australian Government Digital ID System;

(d) for a relying party—the services the relying party is approved to provide, or to provide access to, within the Australian Government Digital ID System;

(e) for an accredited entity—the accredited services of the entity that the entity must provide within the Australian Government Digital ID System;

(f) actions that the entity must take before the entity's approval to participate in the Australian Government Digital ID System is suspended or revoked.

Note 1: For the purposes of paragraph (b), the Digital ID Regulator must have regard to the matters in subsection 63(2) before authorising an entity to collect or disclose restricted attributes of individuals within the Australian Government Digital ID System. If the Digital ID Regulator gives such an authorisation, the Digital ID Regulator must publish a statement of reasons (see subsection 63(3)).

Note 2: An accredited entity may contravene a civil penalty provision of this Act if it discloses a restricted attribute of an individual and the accredited entity's conditions on accreditation do not authorise the disclosure (see subsection 43(2)).

Note 3: A participating relying party may contravene a civil penalty provision of this Act if it collects a restricted attribute of an individual within the Australian Government Digital ID System and the participating relying party's conditions on approval do not authorise this (see subsection 43(3)).

*Conditions imposed by the Digital ID Rules*

(6) The Digital ID Rules may determine that the approval of each entity, or of each entity included in a specified class, to participate in the Australian Government Digital ID System is subject to one or more specified conditions.

(7) Without limiting subsection (6), the Digital ID Regulator may impose conditions that relate to the matters mentioned in subsection (5).

Note: The Minister must have regard to the matters in subsection 63(5) before making Digital ID Rules that authorise participating relying parties to collect or disclose restricted attributes of individuals within the Australian Government Digital ID System.

## 63 Conditions relating to restricted attributes of individuals

*Matters to which the Digital ID Regulator must have regard before authorising disclosure etc. of restricted attributes*

(1) Subsection (2) applies if the Digital ID Regulator proposes to impose a condition on an entity's approval to participate in the Australian Government Digital ID System authorising the entity:

(a) to collect or disclose a restricted attribute of an individual within the Australian Government Digital ID System; or

(b) to disclose a restricted attribute of an individual that is collected by the entity within the Australian Government Digital ID System to an entity outside the system.

(2) In deciding whether to impose the condition, the Digital ID Regulator must have regard to the following matters:

(a) whether the entity has provided sufficient justification for the need to collect or disclose the restricted attribute;

(b) whether the entity has demonstrated that a similar outcome cannot be achieved without collecting or disclosing the restricted attribute;

(c) if the collection or disclosure of the restricted attribute is regulated by other legislative or regulatory requirements—whether the entity has demonstrated that it can comply with those requirements;

(d) the potential harm that could result if restricted attributes of that kind were disclosed to an entity that was not authorised to collect them;

(e) community expectations as to whether restricted attributes of that kind should be handled more securely than other kinds of attributes;

(f) any of the following information provided by the entity seeking authorisation to collect or disclose the restricted attribute:

(i) the entity's risk assessment plan as it relates to the restricted attribute;

(ii) the entity's privacy impact assessment as it relates to the restricted attribute;

(iii) the effectiveness of the entity's protective security (including security governance, information security, personnel security and physical security), privacy arrangements and fraud control arrangements;

(iv) if the entity is not a participating relying party—the arrangements in place between the entity and relying parties for the protection of the restricted attribute from further disclosure;

(g) any other matter the Digital ID Regulator considers relevant.

*Requirement to give statement of reasons if authorisation given*

(3) If the Digital ID Regulator imposes the condition authorising the entity to collect or disclose a restricted attribute of an individual, the Digital ID Regulator must publish on the Digital ID

Regulator's website a statement of reasons for giving the authorisation.

*Matters to which the Minister must have regard before authorising disclosure etc. of restricted attributes*

(4) Subsection (5) applies if the Minister proposes to make Digital ID Rules for the purposes of subsection 62(6) providing that specified kinds of entities are authorised to collect or disclose specified kinds of restricted attributes of individuals, either generally or in specified circumstances.

(5) In deciding whether to make the Digital ID Rules, the Minister must have regard to the following matters:

(a) the potential harm that could result if restricted attributes of that kind were disclosed to an entity;

(b) community expectations as to whether restricted attributes of that kind should be handled more securely than other kinds of attributes;

(c) whether disclosure of restricted attributes of that kind is regulated by another law of the Commonwealth;

(d) any privacy impact assessment that has been conducted in relation to the proposal to make the rules;

(e) any other matter the Minister considers relevant.

## 64 Variation and revocation of conditions

(1) The Digital ID Regulator may vary or revoke a condition imposed on an entity's approval under subsection 62(2):

(a) at any time, on the Digital ID Regulator's own initiative; or

(b) on application by the entity under section 65;

if the Digital ID Regulator considers it is appropriate to do so.

(2) Without limiting subsection (1), the Digital ID Regulator may have regard to the following matters when considering whether it is appropriate to vary or revoke a condition:

(a) matters relating to the security, reliability and stability of the Australian Government Digital ID System;

(b) matters relating to security (within the meaning of the *Australian Security Intelligence Organisation Act 1979*).

### 65 Applying for variation or revocation of conditions on approval

(1) An entity that holds an approval to participate in the Australian Government Digital ID System may apply for a condition imposed on the approval to be varied or revoked.

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

(2) If, after receiving an application under subsection (1), the Digital ID Regulator refuses to vary or revoke a condition, the Digital ID Regulator must give to the entity written notice of the refusal, including reasons for the refusal.

### 66 Notice before changes to conditions on approval

(1) The Digital ID Regulator must not, on the Digital ID Regulator's own initiative:

(a) impose a condition under subsection 62(2) on an entity's approval to participate in the Australian Government Digital ID System after the approval has been given; or

(b) vary or revoke a condition imposed under subsection 64(1);

unless the Digital ID Regulator has given the entity a written notice in accordance with subsection (2).

(2) The notice must:

(a) state the proposed condition, variation or revocation; and

(b) request the entity to give the Digital ID Regulator, within the period specified in the notice, a written statement relating to the proposed condition, variation or revocation.

(3) The Digital ID Regulator must consider any written statement given within the period specified in the notice before making a decision to:

(a) impose a condition under subsection 62(2) on an entity's approval to participate in the Australian Government Digital ID System; or

(b) vary or revoke a condition under subsection 64(1) on an entity's approval to participate in the Australian Government Digital ID System.

(4) This section does not apply if the Digital ID Regulator reasonably believes that the need to impose, vary or revoke the condition is serious and urgent.

(5) If this section does not apply to an entity because of subsection (4), the Digital ID Regulator must give a written statement of reasons to the entity as to why the Digital ID Regulator reasonably believes that the need to impose, vary or revoke the condition is serious and urgent.

(6) The statement of reasons must be given within 7 days after the condition is imposed, varied or revoked.

## 67 Notice of decision of changes of conditions on approval

(1) Subject to subsection (2), the Digital ID Regulator must give an entity written notice of a decision to impose, vary or revoke a condition on an entity's approval to participate in the Australian Government Digital ID System.

(2) The Digital ID Regulator is not required to give an entity notice of the decision if notice of the condition was given in a notice under subsection 59(5).

(3) The notice must:

(a) state the condition or the variation, or state that the condition is revoked; and

(b) state the day on which the condition, variation or revocation takes effect.

## Division 3—Varying, suspending and revoking approval to participate

### 68 Varying approval to participate in the Australian Government Digital ID System

The Digital ID Regulator may vary an approval given to an entity under section 59 to take account of a change in the entity's name.

Note: The Digital ID Regulator can also vary conditions on an approval to participate (see section 64).

### 69 Suspension of approval to participate in the Australian Government Digital ID System

*Digital ID Regulator must suspend approval if Minister's direction is in force*

(1) The Digital ID Regulator must, in writing, suspend an approval given to an entity under section 59 if a direction under subsection 60(2) is in force in relation to the entity.

*Digital ID Regulator may suspend approval in other circumstances*

(2) The Digital ID Regulator may, in writing, suspend an approval given to an entity under section 59 if:

(a) the Digital ID Regulator reasonably believes that the entity has contravened or is contravening this Act; or

(b) the Digital ID Regulator reasonably believes that there has been a cyber security incident involving the entity; or

(c) the Digital ID Regulator reasonably believes that a cyber security incident involving the entity is imminent; or

(d) the Digital ID Regulator reasonably believes that, for reasons of security (within the meaning of the *Australian Security Intelligence Organisation Act 1979*), including on the basis of an adverse or qualified security assessment in respect of a person, it is appropriate to do so; or

(e) if the entity is a body corporate—the entity is a Chapter 5 body corporate (within the meaning of the *Corporations Act 2001*); or

(f) if the entity is an individual—the entity is an insolvent under administration; or

(g) the Digital ID Regulator is satisfied that it is not appropriate for the entity to participate in the Australian Government Digital ID System; or

(h) circumstances specified in the Digital ID Rules apply in relation to the entity.

Note: The Digital ID Regulator may impose conditions on an entity's approval before suspending it (see paragraph 62(5)(f)) and can give directions to an entity to give effect to a decision to suspend an entity's approval (see paragraph 123(1)(b)).

(3) In determining whether the Digital ID Regulator is satisfied of the matter in paragraph (2)(g), regard may be had to whether the entity is a fit and proper person.

Note: In having regard to whether an entity is a fit and proper person, the Digital ID Regulator must have regard to any matters specified in the Digital ID Rules and may have regard to any other matters considered relevant (see section 12).

(4) Subsection (3) does not limit paragraph (2)(g).

*Digital ID Regulator may suspend approval on application*

(5) The Digital ID Regulator may, on application by an entity, suspend an approval given to the entity under section 59.

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

*Show cause notice must generally be given before decision to suspend*

(6) Before suspending the approval of an entity under subsection (2), the Digital ID Regulator must give a written notice (a ***show cause notice***) to the entity.

(7) The show cause notice must:

(a) state the grounds on which the Digital ID Regulator proposes to suspend the entity's approval; and

(b) invite the entity to give the Digital ID Regulator, within 28 days after the day the notice is given, a written statement showing cause why the Digital ID Regulator should not suspend the approval.

*Exception—cyber security incident or security*

(8) Subsection (6) does not apply if the suspension is on a ground mentioned in paragraph (2)(b), (c) or (d).

*Notice of suspension*

(9) If the Digital ID Regulator suspends an entity's approval under subsection (1), (2) or (5), the Digital ID Regulator must give the entity a written notice stating the following:

(a) that the entity's approval to participate in the Australian Government Digital ID System is suspended;

(b) the reasons for the suspension;

(c) the day the suspension is to start;

(d) if the approval is suspended for a period—the period of the suspension;

(e) if the approval is suspended until a specified event occurs or action is taken—the event or action;

(f) if the approval is suspended indefinitely—that fact.

Note: An entity whose approval to participate is suspended remains subject to certain obligations under this Act, including in relation to record keeping (see section 129) and the destruction or de-identification of personal information (see section 130). Such entities may also be subject to directions from the Digital ID Regulator (see sections 123 and 124).

*Revocation of suspension*

(10) If the approval of an entity is suspended under subsection (1), the suspension is revoked if the direction referred to in that subsection is revoked.

(11) The Digital ID Regulator may revoke a suspension of an approval of an entity under subsection (2) by written notice to the entity.

(12) The Digital ID Regulator may revoke a suspension of an approval of an entity under subsection (5) by written notice to the entity, if the entity requests the suspension be revoked.

*Effect of suspension*

(13) If the approval of an entity to participate in the Australian Government Digital ID System is suspended under subsection (1), (2) or (5), the entity is taken not to hold the approval while it is suspended.

## 70 Revocation of approval to participate in the Australian Government Digital ID System

*Digital ID Regulator may revoke approval*

(1) The Digital ID Regulator may, in writing, revoke an approval given to an entity under section 59 if:

(a) the Digital ID Regulator reasonably believes that the entity has contravened or is contravening this Act; or

(b) the Digital ID Regulator reasonably believes that there has been a cyber security incident involving the entity; or

(c) the Digital ID Regulator reasonably believes that, for reasons of security (within the meaning of the *Australian Security Intelligence Organisation Act 1979*), including on the basis of an adverse or qualified security assessment in respect of a person, it is appropriate to do so; or

(d) if the entity is a body corporate—the entity is a Chapter 5 body corporate (within the meaning of the *Corporations Act 2001*); or

(e) if the entity is an individual—the entity is an insolvent under administration; or

(f) the Digital ID Regulator is satisfied that it is not appropriate for the entity to participate in the Australian Government Digital ID System; or

(g) circumstances specified in the Digital ID Rules apply in relation to the entity.

Note: The Digital ID Regulator may impose conditions on an entity's approval before revoking it (see paragraph 62(5)(f)) and can give directions to an entity to give effect to a decision to revoke an entity's approval (see paragraph 123(1)(b)).

(2) In determining whether the Digital ID Regulator is satisfied of the matter in paragraph (1)(f), regard may be had to whether the entity is a fit and proper person.

Note: In having regard to whether an entity is a fit and proper person, the Digital ID Regulator must have regard to any matters specified in the Digital ID Rules and may have regard to any other matters considered relevant (see section 12).

(3) Subsection (2) does not limit paragraph (1)(f).

*Revocation on application*

(4) The Digital ID Regulator must, on application by an entity, revoke an approval given to the entity under section 59. The revocation takes effect on the day determined by the Digital ID Regulator.

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

*Show cause notice must generally be given before decision to revoke*

(5) Before revoking the approval of an entity under subsection (1), the Digital ID Regulator must give a written notice (a ***show cause notice***) to the entity.

(6) The show cause notice must:

(a) state the grounds on which the Digital ID Regulator proposes to revoke the entity's approval; and

(b) invite the entity to give the Digital ID Regulator, within 28 days after the day the notice is given, a written statement showing cause why the Digital ID Regulator should not revoke the approval.

*Notice of revocation*

(7) If the Digital ID Regulator revokes an entity's approval under subsection (1) or (4), the Digital ID Regulator must give the entity a written notice stating the following:

(a) that the entity's approval to participate in the Australian Government Digital ID System is to be revoked;

(b) the reasons for the revocation;

(c) the day the revocation is to take effect.

Note: An entity whose approval to participate has been revoked remains subject to certain obligations under this Act, including in relation to record keeping (see section 129) and the destruction or de-identification of personal information (see section 130). Such entities may also be subject to directions from the Digital ID Regulator (see section 123).

*Approval can be revoked even while suspended*

(8) Despite subsection 69(13), the Digital ID Regulator may revoke an entity's approval to participate in the Australian Government Digital ID System under this section even if a suspension is in force under section 69 in relation to the entity.

# Division 4—Other matters relating to the Australian Government Digital ID System

## 71 Creating and using a digital ID is voluntary

*Creating and using a digital ID is voluntary*

(1) A participating relying party must not, as a condition of providing a service or access to a service, require an individual to create or use a digital ID.

*Exceptions*

(2) Subsection (1) does not apply to a service of a participating relying party if:

(a) the service provides access to another service; and

(b) the individual can access the other service without creating or using a digital ID through the Australian Government Digital ID System.

Example: To open a bank account, ABC Bank requires new customers to verify their identity. ABC Bank allows customers to do this in person at each branch of ABC Bank or alternatively by using the bank's online application service, which requires the use of a digital ID. Jacob wants to open a bank account with ABC Bank but he does not wish to use his digital ID to do so. Because Jacob can verify his identity by going to his nearest branch instead, ABC Bank does not contravene subsection (1).

(3) Subsection (1) does not apply if:

(a) a law of the Commonwealth, a State or a Territory requires verification of the individual's identity solely by means of a digital ID; or

(b) the participating relying party is providing a service, or access to a service, to an individual who is acting on behalf of another entity in a professional or business capacity;

(c) the participating relying party holds an exemption under subsection (4).

*Exemptions*

(4) Subject to subsection (6), the Digital ID Regulator may, on application by a participating relying party, grant an exemption under this subsection to the participating relying party if the Digital ID Regulator is satisfied that it is appropriate to do so.

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

(5) Without limiting subsection (4), the Digital ID Regulator may be satisfied that it is appropriate to grant an exemption if:

(a) the participating relying party is a small business (within the meaning of the *Privacy Act 1988*); or

(b) the participating relying party provides services, or access to services, solely online; or

(c) the participating relying party is providing services, or access to services, in exceptional circumstances.

(6) However, the Digital ID Regulator must not grant an exemption under subsection (4) to a participating relying party that is:

(a) a Commonwealth entity, or a Commonwealth company, within the meaning of the *Public Governance, Performance and Accountability Act 2013*; or

(b) a person or body that is an agency within the meaning of the *Freedom of Information Act 1982*; or

(c) a body specified, or the person holding an office specified, in Part I of Schedule 2 to the *Freedom of Information Act 1982*.

(7) An exemption under subsection (4):

(a) must be in writing; and

(b) may be revoked by the Digital ID Regulator if the Digital ID Regulator considers it appropriate to do so.

(8) The Digital ID Regulator must:

(a) give written notice of a decision to grant, or to refuse to grant, the exemption to the participating relying party; and

(b) if the decision is to refuse to grant the exemption—give reasons for the decision to the participating relying party.

### 72 Notice before exemption is revoked

(1) The Digital ID Regulator must not revoke an exemption granted to an entity under subsection 71(3) unless the Digital ID Regulator has given the entity a written notice in accordance with subsection (2).

(2) The notice must:

(a) state that the Digital ID Regulator proposes to revoke the exemption; and

(b) give reasons for the proposed revocation; and

(c) request the entity to give the Digital ID Regulator, within the period specified in the notice, a written statement relating to the proposed revocation.

(3) The Digital ID Regulator must consider any written statement given within the period specified in the notice before making a decision to revoke the exemption.

(4) This section does not apply if the Digital ID Regulator reasonably believes that the need to revoke the exemption is serious and urgent.

### 73 Holding etc. information outside Australia

(1) The Digital ID Rules may make provision in relation to the holding, storing, handling or transfer of information outside Australia if the information is or was generated, collected, held or stored by accredited entities within the Australian Government Digital ID System.

(2) Without limiting subsection (1), the Digital ID Rules may:

(a) prohibit (either absolutely or unless particular circumstances are met or conditions are complied with) the holding, storing, handling or transferring of such information outside Australia; and

(b) empower the Digital ID Regulator to grant exemptions to entities from any such prohibitions; and

(c) may be expressed to apply to:

(i) entities that hold an approval to participate in the Australian Government Digital ID System; or

(ii) entities whose approval to participate in the Australian Government Digital ID System is suspended; or

(iii) entities whose approval to participate in the Australian Government Digital ID System has been revoked.

(3) An entity is liable to a civil penalty if:

(a) the entity is subject to a requirement under the Digital ID Rules made for the purposes of subsection (1); and

(b) the entity fails to comply with the requirement.

Civil penalty: 300 penalty units.

## 74 Reportable incidents

(1) The Digital ID Rules may prescribe arrangements relating to the notification and management of incidents (***reportable incidents***) that have occurred, or are reasonably suspected of having occurred, in relation to the Australian Government Digital ID System.

Note: The Accreditation Rules may also provide for such arrangements in relation to incidents that occur outside the Australian Government Digital ID System (see subparagraph 27(2)(a)(iv)).

(2) Without limiting subsection (1), the Digital ID Rules may make provision in relation to the following matters:

(a) the entities that are covered by the arrangements;

(b) the kinds of incidents that must be notified;

(c) the information that must be included in notification about reportable incidents;

(d) the manner in which and period within which reportable incidents must be notified to the Digital ID Regulator;

(e) action that must be taken in relation to reportable incidents;

(f) how the Digital ID Regulator deals with reportable incidents, including action that may be taken by the Digital ID Regulator in dealing with a reportable incident such as:

(i) requiring an entity to do something; or

(ii) authorising the provision of information relating to reportable incidents by the Digital ID Regulator to the Minister, the Information Commissioner, accredited entities, participating relying parties or other specified bodies;

(g) authorising the collection of information relating to reportable incidents by the Minister, the Information Commissioner, accredited entities, participating relying parties or other specified bodies.

(3) Without limiting paragraph (2)(b), the Digital ID Rules may specify the following kinds of incidents:

(a) digital ID fraud incidents;

(b) cyber security incidents;

(c) changes in control (within the meaning of section 910B of the *Corporations Act 2001*) of entities covered by the arrangements;

(d) if an accredited entity engages contractors to provide an accredited service, or part of an accredited service, of the entity—changes in relation to such contractors.

(4) An entity is liable to a civil penalty if:

(a) the entity is subject to a requirement under the Digital ID Rules made for the purposes of subsection (1); and

(b) the entity fails to comply with the requirement.

Civil penalty: 300 penalty units.

## 75 Interoperability

(1) The Digital ID Rules may provide for or in relation to requirements relating to the interoperability obligation within the Australian Government Digital ID System.

(2) For the purposes of subsection (1), the ***interoperability obligation*** means:

(a) the obligation on participating relying parties to provide individuals with a choice of accredited identity service

providers when the individual seeks to verify their identity or authenticate their digital ID or other information; and

(b) the obligation on accredited entities participating in the Australian Government Digital ID System to provide their accredited services to other entities participating in the system.

(3) Without limiting subsection (1), the Digital ID Rules may do any of the following:

(a) specify the circumstances in which the interoperability obligation applies to participating relying parties and accredited entities;

(b) provide for the Minister, on application, to grant exemptions from the interoperability obligation;

(c) specify the grounds on which the Minister may grant exemptions, which may include the following:

(i) that the Minister is satisfied that a service, or access to a service, provided by a participating relying party that is a government entity is of a kind that should be provided only to other government entities;

(ii) that the participating relying party provides a service, or access to a service, that the Minister is satisfied is of a kind that would promote use of digital IDs if the service, or access to the service, was available through the Australian Government Digital ID System;

(iii) that the exemption is of a limited duration to allow for the implementation of required business practices or technological systems, or to facilitate the use of the Australian Government Digital ID System by particular kinds of entities;

(iv) that an entity will provide an arrangement to assist individuals who would otherwise be at a disadvantage in accessing the Australian Government Digital ID System;

(v) the exemption is necessary to satisfy the requirements of another legislative provision or scheme;

(vi) that the governance arrangements of an accredited entity prohibit or restrict the entity from interacting with a particular kind of service.

## 76 Service levels for accredited entities and participating relying parties

(1) The Digital ID Standards Chair may, in writing, determine either or both of the following:

(a) service levels relating to the availability and performance of the information technology systems through which accredited entities that hold an approval to participate in the Australian Government Digital ID System will provide their accredited services;

(b) service levels relating to the availability and performance of the services participating relying parties are approved to provide, or provide access to, within the Australian Government Digital ID System.

(2) A determination made under subsection (1) is a legislative instrument, but section 42 (disallowance) of the *Legislation Act 2003* does not apply to the instrument.

## 77 Entities may conduct testing in relation to the Australian Government Digital ID System

(1) The Digital ID Regulator may authorise an entity to conduct testing in relation to the Australian Government Digital ID System for the purposes of determining the entity's capability or suitability to participate in the system.

(2) The authorisation:

(a) must be in writing; and

(b) must specify the period for which it is in force, which must not exceed 3 months; and

(c) may be granted unconditionally or subject to conditions.

Note: The Digital ID Regulator may vary or revoke the authorisation: see subsection 33(3) of the *Acts Interpretation Act 1901*.

(3) If an authorisation under this section is given subject to a condition and the condition is not met at a particular time, the authorisation ceases to be in force at that time.

### 78 Use and disclosure of personal information to conduct testing

(1) An accredited entity may use or disclose personal information of an individual if:

(a) the accredited entity uses or discloses the information for the purposes of conducting testing in relation to the Australian Government Digital ID System; and

(b) the accredited entity or another entity is authorised under section 77 to conduct the testing using the information; and

(c) the individual to whom the information relates has expressly consented to the use or disclosure of the information for that purpose.

(2) This section applies despite anything else in this Act.

# Part 3—Liability and redress framework

## Division 1—Liability of participating entities

### 79 Accredited entities participating in the Australian Government Digital ID System protected from liability in certain circumstances

(1) This section applies if, while participating in the Australian Government Digital ID System, an accredited entity:

(a) provides, or fails to provide, an accredited service of the entity to another accredited entity participating in the Australian Government Digital ID System, or to a participating relying party; and

(b) provides, or fails to provide, the accredited service in good faith, in compliance with this Act.

(2) The accredited entity is not liable to any action or other proceeding, whether civil or criminal, in relation to that accredited service or the provision of that accredited service.

(3) An entity that wishes to rely on subsection (2) in relation to an action or other proceeding bears an evidential burden (within the meaning of the Regulatory Powers Act) in relation to that matter.

## Division 2—Statutory contract

### 80 Statutory contract between entities participating in the Australian Government Digital ID System

(1) A contract is taken to be in force between:

(a) an accredited entity and each other accredited entity; and

(b) an accredited entity and each participating relying party;

under which each accredited entity agrees to:

(c) provide the entity's accredited services while participating in the Australian Government Digital ID System in compliance with this Act, to the extent it relates to verifying the identity of an individual or authenticating the digital ID of, or information about, an individual; and

(d) comply with requirements in relation to intellectual property rights that are prescribed by the Digital ID Rules for the purposes of this paragraph.

Note 1: This means an accredited entity will be taken to have a separate contract with each other accredited entity and with each participating relying party.

Note 2: The Digital ID Rules may provide that some provisions of this Act (which is defined to include the Digital ID Data Standards and other legislative instruments) are not covered by the contract (see subsection (5)).

(2) The contract is taken to be in force during the period:

(a) starting on the day that the participation start day for both entities has arrived or passed; and

(b) ending on the day on which the approval to participate in the Australian Government Digital ID System has been revoked for one or both of the entities.

(3) If an accredited entity breaches the contract, an application to the Federal Circuit and Family Court of Australia (Division 2) may be made by the party to the contract that has suffered, or is likely to suffer, loss or damage as a result of the breach.

(4) After giving an opportunity to be heard to the applicant and the entity (the ***respondent***) against whom the order is sought, the Federal Circuit and Family Court of Australia (Division 2) may make any or all of the following orders:

(a) an order giving directions to the respondent about compliance with, or enforcement of, the contract;

(b) an order directing the respondent to compensate the entity that has suffered loss or damage as a result of the breach;

(c) an order directing the respondent to prevent or reduce loss or damage suffered, or likely to be suffered;

(d) any other order that the Court considers appropriate.

(5) The Digital ID Rules may make provision in relation to the following matters:

(a) conduct or circumstances that do, or do not, constitute breaches of contract;

(b) provision of this Act that are not covered by the contract;

(c) limits on the kinds of losses or damages for which compensation may be payable;

(d) limits on the amount of compensation that an accredited entity may be liable to pay.

## 81 Participating entities to maintain insurance as directed by Digital ID Regulator

(1) The Digital ID Regulator may, in writing, direct an accredited entity that is participating in the Australian Government Digital ID System to maintain adequate insurance against any liabilities arising in connection with the obligations under section 80.

(2) If the Digital ID Regulator gives a direction to an entity under subsection (1), the direction is taken to be a condition imposed under subsection 62(2) on the entity's approval to participate in the Australian Government Digital ID System.

(3) A direction given under this section is not a legislative instrument.

## 82 Dispute resolution procedures

The Digital ID Rules may make provision for and in relation to dispute resolution procedures that must be complied with before an entity can apply for an order under subsection 80(3).

# Division 3—Redress framework

## 83 Redress framework

(1) The Digital ID Rules may 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 Government Digital ID System.

(2) Without limiting subsection (1), the redress framework may deal with the following matters:

(a) the entities that are covered by the framework;

(b) the kinds of incidents that are covered by the framework, which may include digital ID fraud incidents and cyber security incidents;

(c) procedures for dealing with incidents that are covered by the framework;

(d) requirements relating to notifying entities affected by incidents covered by the framework;

(e) the provision of information, support and assistance to entities affected by incidents covered by the framework;

(f) development and publication of policies relating to the identification, management and resolution of incidents covered by the framework.

# Chapter 5—Digital ID Regulator

## Part 1—Introduction

### 84 Simplified outline of this Chapter

# Part 2—Digital ID Regulator

## 85 Digital ID Regulator

The Digital ID Regulator is the Australian Competition and Consumer Commission.

Note: The Australian Competition and Consumer Commission is established by Part II of the *Competition and Consumer Act 2010*.

## 86 Functions of the Digital ID Regulator

*Consultation note:*

The Bill will set out the functions of the Digital ID Regulator. These functions primarily relate to the regulation of accredited entities and other entities participating as relying parties in the Australian Government Digital ID System. The Bill sets out other more operational functions relating to ensuring the integrity and performance of the Australian Government Digital ID System which are currently performed by Services Australia.

The sharing of these functions between the Digital ID Regulator and Services Australia remains under consideration.

Below is a description of the current intention for the sharing of functions between Australian Competition and Consumer Commission as the Digital ID Regulator and the Chief Executive Officer of Services Australia as administrator of the Australian Government Digital ID System.

Digital ID Regulator:

- the functions conferred on the Digital ID Regulator by or under the Act involving accreditation, approvals to participate in the Australian Government Digital ID System and

| |
|---|
| enforcement, other than where those functions are conferred on Services Australia<br><br>· advising the Finance Minister on matters relating to any of the Digital ID Regulator's functions<br><br>· anything that is incidental or conducive to the performance of any of the above functions.<br><br>Services Australia: administering the operation of the Australian Government Digital ID System:<br><br>· identifying and managing risks in relation to the Australian Government Digital ID System<br><br>· managing Digital ID fraud incidents and cyber security incidents that affect the Australian Government Digital ID System<br><br>· advising the Finance Minister or the Digital ID Regulator on matters relating to the operation of the Australian Government Digital ID System<br><br>· anything that is incidental or conducive to the performance of any of the above functions. |

## 87 Powers of the Digital ID Regulator

The Digital ID Regulator has power to do all things necessary or convenient to be done for or in connection with the performance of the Regulator's functions under this Act.

# Division 2—Confidentiality obligations of the Digital ID Regulator and certain other persons

## 88 Prohibition on entrusted persons using or disclosing personal or commercially sensitive information

*Offence*

(1) A person commits an offence if:

(a) the person is or has been an entrusted person; and

(b) the person obtains protected information in the course of, or for the purposes of, performing functions or exercising powers under this Act; and

(c) the person uses or discloses the information; and

(d) either of the following applies:

(i) the information is personal information about an individual;

(ii) there is a risk that the use or disclosure might substantially prejudice the commercial interests of another person.

Penalty: Imprisonment for 2 years or 120 penalty units, or both.

(2) An ***entrusted person*** means:

(a) the Digital ID Regulator; or

(b) a member of the Commission (within the meaning of the *Competition and Consumer Act 2010*); or

(c) an associate member of the Australian Competition and Consumer Commission; or

(d) a member of the staff of the Australian Competition and Consumer Commission; or

(e) a person engaged under section 27A of the *Competition and Consumer Act 2010*.

*Exception—authorised use or disclosure*

(3) Subsection (1) does not apply if the use or disclosure is authorised by section 89 (authorised uses and disclosures).

Note: A defendant bears an evidential burden in relation to a matter in this subsection (see subsection 13.3(3) of the *Criminal Code*).

*Definition of protected information*

(4) ***Protected information*** means information that was disclosed or obtained under or for the purposes of this Act.

### 89 Authorised uses and disclosures of personal or commercially sensitive information by entrusted persons

(1) An entrusted person may use or disclose protected information if:

(a) the use or disclosure is made for the purposes of:

(i) performing a duty or function, or exercising a power, under or in relation to this Act; or

(ii) enabling another person to perform duties or functions, or exercise powers, under or in relation to this Act; or

(iii) assisting in the administration or enforcement of another law of the Commonwealth, or of a State or Territory; or

(b) the use or disclosure is required or authorised by or under:

(i) a law of the Commonwealth (including this Act); or

(ii) a law of a State or Territory that is prescribed by the Digital ID Rules; or

(c) the person referred to in subparagraph 88(1)(d)(i) or (ii) has expressly consented to the use or disclosure; or

(d) at the time of the use or disclosure, the protected information is already lawfully publicly available; or

(e) both:

(i) the use or disclosure is, or is a kind of use or disclosure that is, certified in writing by the Minister to be in the public interest; and

(ii) the use or disclosure is made in accordance with any requirements prescribed by the Digital ID Rules; or

(f) both:

(i) the entrusted person believes on reasonable grounds that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of a person; and

(ii) the use or disclosure is for the purposes of preventing or lessening that threat.

(2) An instrument made under subparagraph (1)(e)(i) certifying that a particular use or disclosure is in the public interest is not a legislative instrument.

(3) An instrument made under subparagraph (1)(e)(i) certifying that a kind of use or disclosure is in the public interest is a legislative instrument.

### 90 Disclosing personal or commercially sensitive information to courts and tribunals etc. by entrusted persons

(1) Except where it is necessary to do so for the purposes of giving effect to this Act, an entrusted person is not to be required:

(a) to produce a document containing protected information to a body mentioned in subsection (2); or

(b) to disclose protected information to such a body;

if either of the following applies:

(c) the information is personal information of an individual other than the entrusted person;

(d) there is a risk that production of the document or disclosure of the information might substantially prejudice the commercial interests of a person.

(2) The bodies are a court, tribunal, authority or other person having power to require the production of documents or the answering of questions.

# Part 2—Advisory committees

## 91 Advisory committees

(1) The Minister may establish, in writing, such advisory committees as the Minister considers appropriate to provide advice to the following in relation to the performance of the Digital ID Regulator's functions and exercise of the Regulator's powers under this Act:

(a) the Minister;

(b) the Secretary;

(c) the Digital ID Data Standards Chair.

(2) An advisory committee is to consist of such persons as the Minister determines.

(3) If the Minister establishes an advisory committee under subsection (1), the Minister must, in writing, determine:

(a) the committee's terms of reference; and

(b) the terms and conditions of appointment of the members of the committee, including:

(i) term of office; and

(ii) remuneration; and

(iii) allowances; and

(iv) leave of absence; and

(v) disclosure of interests; and

(vi) termination of membership; and

(c) the procedures to be followed by the committee.

(4) An instrument made under subsection (1) or (3) is not a legislative instrument.

# Chapter 6—Digital ID Data Standards

## Part 1—Introduction

### 92 Simplified outline of this Chapter

# Part 2—Digital ID Data Standards

## 93 Digital ID Data Standards

(1) The Digital ID Standards Chair may, in writing, make one or more standards (***Digital ID Data Standards***) about the following:

(a) technical integration requirements for entities to participate in the Australian Government Digital ID System;

(b) technical or design features that entities must have to participate in the Australian Government Digital ID System;

(c) if required to do so by the Accreditation Rules—technical, data or design standards, including test standards for an entity's information technology systems, relating to accreditation;

(d) other matters prescribed by the Digital ID Rules.

(2) Without limiting subsection 33(3A) of the *Acts Interpretation Act 1901*, Digital ID Data Standards may provide differently for different kinds of entities, things or circumstances.

(3) Digital ID Data Standards that are inconsistent with the Accreditation Rules have no effect to the extent of the inconsistency, but Digital ID Data Standards are taken to be consistent with the Accreditation Rules to the extent that Digital ID Data Standards are capable of operating concurrently with the Accreditation Rules.

(4) Digital ID Data Standards are legislative instruments, but section 42 (disallowance) of the *Legislation Act 2003* does not apply to them.

## 94 Requirement to consult before making

(1) Before making or amending Digital ID Data Standards under section 93, the Digital ID Data Standards Chair must:

(a) consult the Minister;

(b) cause to be published on the Department's website a notice:
(i) setting out the draft standards or amendments; and
(ii) inviting persons to make submissions to the Chair about the draft standards or amendments within the period specified in the notice (which must be at least 28 days after the notice is published); and
(c) consider any submissions received within the specified period.

(2) The Digital ID Data Standards Chair may consider any submissions received after the specified period if the Chair considers it appropriate to do so.

(3) Before making or amending Digital ID Data Standards under section 93, the Digital ID Data Standards Chair may consult:
(a) the Digital ID Regulator; or
(b) the Information Commissioner.

(4) This section does not limit section 17 of the *Legislation Act 2003* (rule-makers should consult before making legislative instrument).

# Part 3—Digital ID Data Standards Chair

## Division 1—Establishment and functions of the Digital ID Data Standards Chair

### 95 Data Standards Chair

There is to be a Digital ID Data Standards Chair.

### 96 Functions of the Digital ID Data Standards Chair

The functions of the Digital ID Data Standards Chair are:

(a) to make Digital ID Data Standards; and

(b) to review those standards regularly; and

(c) such other functions as are conferred on the Chair by this Act; and

(d) to do anything incidental or conducive to the performance of any of the above functions.

### 97 Powers of the Digital ID Data Standards Chair

The Digital ID Data Standards Chair has the power to do all things necessary or convenient to be done for or in connection with the performance of the Chair's functions.

### 98 Directions to the Digital ID Data Standards Chair

(1) The Minister may give written directions to the Digital ID Data Standards Chair about the performance of the Chair's functions and the exercise of the Chair's powers.

(2) A direction under subsection (1) must be of a general nature only.

(3) The Digital ID Data Standards Chair must comply with a direction under subsection (1).

(4) A direction under subsection (1) is not a legislative instrument.

# Division 2—Appointment of the Digital ID Data Standards Chair

## 99 Appointment

(1) The Digital ID Data Standards Chair is to be appointed by the Minister by written instrument.

Note: The Minister will be the Digital ID Data Standards Chair in the absence of an appointment under this section (see the definition of ***Digital ID Data Standards Chair*** in section 9).

(2) The Digital ID Data Standards Chair is to be appointed on a full-time or part-time basis.

## 100 Term of appointment

The Digital ID Data Standards Chair holds office for the period specified in the instrument of appointment. The period must not exceed 3 years.

Note: The Digital ID Data Standards Chair may be reappointed: see section 33AA of the *Acts Interpretation Act 1901*.

## 101 Acting appointments

The Minister may, by written instrument, appoint a person to act as the Digital ID Data Standards Chair:

(a) during a vacancy in the office of Digital ID Data Standards Chair (whether or not an appointment has previously been made to the office); or

(b) during any period, or during all periods, when the Digital ID Data Standards Chair:

(i) is absent from duty or from Australia; or

(ii) is, for any reason, unable to perform the duties of the office.

Note: For rules that apply to acting appointments, see sections 33AB and 33A of the *Acts Interpretation Act 1901*.

### 102 Application of the finance law etc.

(1) For the purposes of the finance law (within the meaning of the *Public Governance, Performance and Accountability Act 2013*), the Digital ID Data Standards Chair is an official of the Department.

Note: A consequence of this subsection is that the Secretary of the Department is the accountable authority (within the meaning of that Act) applicable to the Digital ID Data Standards Chair.

(2) The Secretary of the Department, when preparing the Department's annual report under section 46 of the *Public Governance, Performance and Accountability Act 2013* for a period, must include information in that report about:

(a) the performance of the Digital ID Data Standards Chair's functions; and

(b) the exercise of the Digital ID Data Standards Chair's powers;

during the period.

(3) If at any time the Digital ID Data Standards Chair is the Minister then:

(a) subsections (1) and (2) do not apply during that time; and

(b) the Department's annual report under section 46 of the *Public Governance, Performance and Accountability Act 2013* for the period that includes that time must include information about the performance of the Digital ID Data Standards Chair's functions, and the exercise of the Digital ID Data Standards Chair's powers, at that time.

# Division 3—Terms and conditions for the Digital ID Data Standards Chair

## 103 Remuneration

(1) The Digital ID Data Standards Chair is to be paid the remuneration that is determined by the Remuneration Tribunal. If no determination of that remuneration by the Tribunal is in operation, the Digital ID Data Standards Chair is to be paid the remuneration that is prescribed by legislative instrument under subsection (3).

(2) The Digital ID Data Standards Chair is to be paid the allowances that are prescribed by legislative instrument under subsection (3).

(3) The Minister may, by legislative instrument, prescribe:

(a) remuneration for the purposes of subsection (1); and

(b) allowances for the purposes of subsection (2).

(4) Subsections (1) and (2) do not apply while the Digital ID Data Standards Chair is the Minister.

(5) Subsections 7(9) and (13) of the *Remuneration Tribunal Act 1973* do not apply in relation to the office of the Digital ID Data Standards Chair.

Note: The effect of this subsection is that remuneration or allowances of the Digital ID Data Standards Chair will be paid out of money appropriated by an Act other than the *Remuneration Tribunal Act 1973*.

(6) This section has effect subject to the *Remuneration Tribunal Act 1973* (except as provided by subsection (5) of this section).

## 104 Leave of absence

(1) If the Digital ID Data Standards Chair is appointed on a full-time basis, the Data Standards Chair has the recreation leave entitlements that are determined by the Remuneration Tribunal.

(2) If the Digital ID Data Standards Chair is appointed on a full-time basis, the Minister may grant the Data Standards Chair leave of absence, other than recreation leave, on the terms and conditions as to remuneration or otherwise that the Minister determines.

(3) If the Digital ID Data Standards Chair is appointed on a part-time basis, the Secretary of the Department may grant leave of absence to the Data Standards Chair on the terms and conditions that the Secretary determines.

## 105 Outside work

The Digital ID Data Standards Chair must not engage in paid work outside the duties of the Digital ID Data Standards Chair's office without the Minister's approval.

## 106 Disclosure of interests

(1) The Digital ID Data Standards Chair must give written notice to the Minister of any direct or indirect pecuniary interest that the Digital ID Data Standards Chair has or acquires and that conflicts or could conflict with the proper performance of the Digital ID Data Standards Chair's functions.

(2) Subsection (1) applies in addition to section 29 of the *Public Governance, Performance and Accountability Act 2013* (which deals with the duty to disclose interests).

## 107 Resignation of appointment

*Resignation*

(1) The Digital ID Data Standards Chair may resign the Digital ID Data Standards Chair's appointment by giving the Minister a written resignation.

(2) The resignation takes effect on the day it is received by the Minister or, if a later day is specified in the resignation, on that later day.

### 108 Termination of appointment

(1) The Minister may terminate the appointment of the Digital ID Data Standards Chair:

(a) for misbehaviour; or

(b) if the Digital ID Data Standards Chair is unable to perform the duties of the Digital ID Data Standards Chair's office because of physical or mental incapacity.

(2) The Minister may terminate the appointment of the Digital ID Data Standards Chair if:

(a) the Digital ID Data Standards Chair:

(i) becomes bankrupt; or

(ii) applies to take the benefit of any law for the relief of bankrupt or insolvent debtors; or

(iii) compounds with the Digital ID Data Standards Chair's creditors; or

(iv) makes an assignment of the Digital ID Data Standards Chair's remuneration for the benefit of the Digital ID Data Standards Chair's creditors; or

(b) if the Digital ID Data Standards Chair is appointed on a full-time basis—the Digital ID Data Standards Chair is absent, except on leave of absence, for 14 consecutive days or for 28 days in any 12-month period; or

(c) the Digital ID Data Standards Chair fails, without reasonable excuse, to comply with section 29 of the *Public Governance, Performance and Accountability Act 2013* (which deals with the duty to disclose interests) or rules made for the purposes of that section.

### 109 Other terms and conditions

(1) The Digital ID Data Standards Chair holds office on the terms and conditions (if any) in relation to matters not covered by this Division that are determined by the Minister.

(2) Subsection (1) does not apply while the Digital ID Data Standards Chair is the Minister.

# Division 4—Other matters

## 110 Arrangements relating to staff

(1) The staff assisting the Digital ID Data Standards Chair are to be APS employees in the Department whose services are made available to the Chair, by the Secretary, in connection with the performance of any of the Chair's functions or the exercise of any of the Chair's powers.

(2) When performing services for the Digital ID Data Standards Chair, the staff are subject to the directions of the Chair.

## 111 Consultants

(1) The Digital ID Data Standards Chair may, on behalf of the Commonwealth, engage consultants to assist in the performance of the Chair's functions or the exercise of the Chair's powers.

(2) The consultants are to be engaged on the terms and conditions that the Digital ID Data Standards Chair determines in writing.

# Chapter 7—Trustmarks and registers

## Part 1—Introduction

### 112 Simplified outline of this Chapter

# Part 2—Digital ID trustmarks

## 113 Digital ID trustmarks

(1) The Digital ID Rules may do one or more of the following:

(a) specify one or more digital ID trustmarks that may or must be used by accredited entities;

(b) specify one or more digital ID trustmarks that may or must be used by participating relying parties;

(c) prescribe conditions or requirements in relation to the use or display of those digital ID trustmarks.

(2) ***Digital ID trustmark*** means a mark, symbol, logo or design set out in the Digital ID Rules.

## 114 Authorised use of digital ID trustmarks etc.

(1) An entity is authorised to use a digital ID trustmark if:

(a) the Digital ID Rules permit or require the entity to use the digital ID trustmark; and

(b) if the Digital ID Rules prescribe conditions in relation to the use or display of the digital ID trustmark—the entity complies with the conditions.

(2) An entity must not use a digital ID trustmark if the entity is not authorised under subsection (1) to use the trustmark.

Civil penalty: 200 penalty units.

(3) An entity must not do any of the following in relation to a mark, symbol, logo or design so closely resembling a digital ID trustmark as to be likely to lead a reasonable person to believe that the entity is an accredited entity or a participating relying party:

(a) use it in relation to a business, trade, profession or occupation;

(b) apply (as a trade mark or otherwise) it to goods imported, manufactured, produced, sold, offered for sale or let on hire;

(c) use it in relation to:
(i) goods or services; or
(ii) the promotion (by any means) of the supply or use of goods or services.

Civil penalty: 200 penalty units.

### 115 Displaying digital ID trustmark

An entity contravenes this subsection if:
(a) the entity is required by the Digital ID Rules to display a digital ID trustmark in circumstances specified in the Digital ID Rules; and
(b) the entity fails to comply with the requirement.

Civil penalty: 200 penalty units.

# Part 3—Registers

## 116 Digital ID Accredited Entities Register

(1) The Digital ID Regulator must establish and maintain a register (the ***Digital ID Accredited Entities Register***) of entities who are, or have been, accredited entities.

(2) The Digital ID Accredited Entities Register must contain the following details for each entity:

(a) the kinds of accredited entity that the entity is accredited as and the day on which each accreditation came into force;

(b) any conditions imposed on the accreditation under subsection 18(2) that are in force, including any variations to those conditions, and the day the condition or variation took effect;

(c) any conditions imposed on the accreditation under subsection 18(2) that have been revoked, and the day the revocation took effect;

(d) if the entity's accreditation is or has been suspended for a period—that fact and the period of the suspension;

(e) if the entity's accreditation is or has been suspended until a specified event occurs or action is taken—that fact and the event or action;

(f) if the entity's accreditation is or has been suspended indefinitely—that fact;

(g) if the entity's accreditation has been revoked—that fact, and the date the revocation took effect;

(h) any other information prescribed by the Digital ID Rules.

(3) The Digital ID Accredited Entities Register may contain any other information that the Digital ID Regulator considers appropriate.

(4) If an entity's accreditation is revoked and the entity does not become an accredited entity again for 12 months after the day the revocation came into force, the Digital ID Regulator must remove

the entity from the Digital ID Accredited Entities Register at the end of that period.

(5) The Digital ID Rules may make provision for and in relation to the following:

(a) the correction of information in the Digital ID Accredited Entities register;

(b) any other matter relating to the administration or operation of the Digital ID Accredited Entities Register.

(6) The Digital ID Accredited Entities Register must be made publicly available on the Digital ID Regulator's website.

(7) The Digital ID Accredited Entities Register is not a legislative instrument.

## 117 AGDIS Register

(1) The Digital ID Regulator must establish and maintain a register (the ***AGDIS Register***) of entities who are participating in the Australian Government Digital ID System.

(2) The AGDIS Register must contain the following details for each entity:

(a) the day the entity's approval to participate in the Australian Government Digital ID System came into force;

(b) the entity's participation start day;

(c) if the entity is a participating relying party:

(i) each service the participating relying party is approved to provide, or to provide access to, within the Australian Government Digital ID System;

(ii) if the participating relying party provides, or may provide, attributes of individuals obtained from the Australian Government Digital ID System to other relying parties—details of those other relying parties, including the services the other relying parties provide, or provide access to;

(d) if the entity is an accredited entity—the kind of accredited entity it is accredited as;

(e) any conditions imposed on the entity's approval to participate under subsection 62(2) that are in force, including any variations to those conditions, and the day the condition or variation took effect;

(f) any conditions imposed on the entity's approval to participate under subsection 62(2) that have been revoked, and the day the revocation took effect;

(g) if the entity's approval to participate is or has been suspended for a period—that fact and the period of the suspension;

(h) if the entity's approval to participate is or has been suspended until a specified event occurs or action is taken—that fact and the event or action;

(i) if the entity's approval to participate is or has been suspended indefinitely—that fact;

(j) if the entity's approval to participate has been revoked—that fact, and the date the revocation took effect;

(k) any other information prescribed by the Digital ID Rules.

(3) The AGDIS Register may contain any other information that the Digital ID Regulator considers appropriate.

(4) If an entity's approval to participate in the Australian Government Digital ID System is revoked, and the entity does not hold another approval to participate in the Australian Government Digital ID System for 3 years after the day the revocation came into force, the Digital ID Regulator must remove the entity from the AGDIS Register at the end of that period.

(5) The Digital ID Rules may make provision for and in relation to the following:

(a) the correction of information in the AGDIS Register;

(b) any other matter relating to the administration or operation of the AGDIS Register.

(6) The AGDIS Register must be made publicly available on the Digital ID Regulator's website.

(7) The AGDIS Register is not a legislative instrument.

# Chapter 8—Administration

## Part 1—Introduction

### 118 Simplified outline of this Chapter

# Part 2—Compliance and enforcement

## Division 1—Enforcement powers

### 119 Civil penalty provisions

*Enforceable civil penalty provisions*

(1) Each civil penalty provision of this Act is enforceable under Part 4 of the Regulatory Powers Act.

Note: Part 4 of the Regulatory Powers Act allows a civil penalty provision to be enforced by obtaining an order for a person to pay a pecuniary penalty for the contravention of the provision.

*Authorised applicant*

(2) For the purposes of Part 4 of the Regulatory Powers Act:

(a) the Information Commissioner or a member of staff of the Office of the Australian Information Commissioner who is an SES employee or acting SES employee are authorised applicants in relation to the civil penalty provisions in Division 2 of Part 2 of Chapter 3 of this Act (about additional privacy safeguards); and

(b) the Digital ID Regulator is an authorised applicant in relation to every other civil penalty provision of this Act.

*Relevant court*

(3) For the purposes of Part 4 of the Regulatory Powers Act, each of the following courts is a relevant court in relation to the civil penalty provisions of this Act:

(a) the Federal Court of Australia;

(b) the Federal Circuit and Family Court of Australia (Division 2);

(c) a court of a State or Territory that has jurisdiction in relation to the matter.

## 120 Infringement notices

*Provisions subject to an infringement notice*

(1) Each civil penalty provision of this Act is subject to an infringement notice under Part 5 of the Regulatory Powers Act.

Note: Part 5 of the Regulatory Powers Act creates a framework for using infringement notices in relation to provisions.

*Infringement officer*

(2) For the purposes of Part 5 of the Regulatory Powers Act:

(a) the Information Commissioner or a member of staff of the Office of the Australian Information Commissioner who is an SES employee or acting SES employee are infringement officers in relation to the civil penalty provisions in Division 2 of Part 2 of Chapter 3 of this Act (about additional privacy safeguards); and

(b) the Digital ID Regulator is an infringement officer in relation to every other civil penalty provision of this Act.

*Relevant chief executive*

(3) For the purposes of Part 5 of the Regulatory Powers Act, the relevant chief executive is:

(a) in relation to the provisions mentioned in paragraph (2)(a) of this section—the Information Commissioner; and

(b) in relation to the provisions mentioned in paragraph (2)(b) of this section—the Digital ID Regulator.

## 121 Enforceable undertakings

*Enforceable provisions*

(1) Each civil penalty provision of this Act is enforceable under Part 6 of the Regulatory Powers Act.

Note: Part 6 of the Regulatory Powers Act creates a framework for accepting and enforcing undertakings relating to compliance with provisions.

*Authorised person*

(2) For the purposes of Part 6 of the Regulatory Powers Act:

(a) the Information Commissioner is an authorised person in relation to the civil penalty provisions in Division 2 of Part 2 of Chapter 3 of this Act (about additional privacy safeguards); and

(b) the Digital ID Regulator is an authorised person in relation to every other civil penalty provision of this Act.

*Relevant court*

(3) For the purposes of Part 6 of the Regulatory Powers Act, each of the following courts is a relevant court in relation to the provisions mentioned in subsection (1):

(a) the Federal Court of Australia;

(b) the Federal Circuit and Family Court of Australia (Division 2);

(c) a court of a State or Territory that has jurisdiction in relation to the matter.

*Publishing undertakings*

(4) The Information Commissioner may publish an undertaking accepted by the Information Commissioner on the Information Commissioner's website.

(5) The Digital ID Regulator may publish an undertaking accepted by the Regulator on the Regulator's website.

## 122 Injunctions

*Enforceable provisions*

(1) Each civil penalty provision of this Act is enforceable under Part 7 of the Regulatory Powers Act.

Note: Part 7 of the Regulatory Powers Act creates a framework for using injunctions to enforce provisions.

*Authorised person*

(2) For the purposes of Part 7 of the Regulatory Powers Act:

(a) the Information Commissioner is an authorised person in relation to the civil penalty provisions in Division 2 of Part 2 of Chapter 3 of this Act (about additional privacy safeguards); and

(b) the Digital ID Regulator is an authorised person in relation to every other civil penalty provision of this Act.

*Relevant court*

(3) For the purposes of Part 7 of the Regulatory Powers Act, each of the following courts is a relevant court in relation to the provisions mentioned in subsection (1):

(a) the Federal Court of Australia;

(b) the Federal Circuit and Family Court of Australia (Division 2);

(c) a court of a State or Territory that has jurisdiction in relation to the matter.

## Division 2—Directions powers

### 123 Digital ID Regulator's power to give directions to entities in relation to participation and accreditation

(1) The Digital ID Regulator may give an entity a direction to do a specified act or thing, or not do a specified act or thing, within the period specified in the direction if the Digital ID Regulator considers it necessary to:

(a) give effect to a decision to approve an entity to participate in the Australian Government Digital ID System; or

(b) give effect to a decision to suspend or revoke an entity's approval to participate in the Australian Government Digital ID System; or

(c) to deal with matters arising as a result of the suspension or revocation of an entity's approval to participate in the Australian Government Digital ID System; or

(d) give effect to a decision to accredit an entity as an accredited entity; or

(e) give effect to a decision to suspend or revoke an entity's accreditation as an accredited entity; or

(f) to deal with matters arising as a result of the suspension or revocation of an entity's accreditation as an accredited entity.

(2) Without limiting subsection (1), a direction may:

(a) require an accredited identity exchange provider to:

(i) provide information to an entity that holds an approval to participate in the Australian Government Digital ID System about the steps required to connect to the system; and

(ii) connect the entity to the Australian Government Digital ID System by a specified date; or

(b) require an entity whose accreditation has been suspended or revoked to notify other participants in the digital ID system in which the entity participates of the suspension or

revocation and the date on which the suspension or revocation takes effect.

(3) The direction must:

(a) be in writing; and

(b) specify the reason for the direction.

(4) An entity must comply with a direction given under subsection (1).

Civil penalty: 200 penalty units.

(5) A direction under subsection (1) is not a legislative instrument.

### 124 Digital ID Regulator's power to give directions to protect the integrity or performance of the Australian Government Digital ID System

(1) The Digital ID Regulator may give a direction to the following entities if the Digital ID Regulator considers it necessary to do so to protect the integrity or performance of the Australian Government Digital ID System:

(a) entities that hold an approval to participate in the Australian Government Digital ID System;

(b) entities whose approval to participate in the Australian Government Digital ID System is suspended;

(c) accredited entities;

(d) entities whose accreditation as an accredited entity is suspended.

(2) Without limiting subsection (1), the Digital ID Regulator may give a direction to do one or more of the following:

(a) conduct a privacy impact assessment in relation to a specified matter and provide a copy of the assessment to the Digital ID Regulator;

(b) conduct a fraud assessment in relation to a specified matter and provide a copy of the report to the Digital ID Regulator in relation to the assessment;

(c) conduct a security assessment in relation to a specified matter and provide a copy of the report to the Digital ID Regulator in relation to the assessment;

(d) an act or thing specified by the Digital ID Rules.

(3) If Accreditation Rules made for the purposes of section 27 prescribe requirements in relation to the conduct of an assessment mentioned in subsection (2), the assessment must comply with the requirements.

(4) The direction must:

(a) be in writing; and

(b) specify the reason for the direction.

(5) An entity must comply with a direction given under subsection (1).

Civil penalty: 200 penalty units.

(6) A direction under subsection (1) is not a legislative instrument.

### 125 Remedial directions to accredited entities etc.

(1) This section applies if the Digital ID Regulator reasonably believes that an accredited entity, or an entity whose accreditation is suspended, has contravened, or is contravening, a provision of this Act.

(2) The Digital ID Regulator may give the entity a direction requiring the entity to take specified action directed towards ensuring that the entity does not contravene the provision, or is unlikely to contravene the provision, in the future.

(3) The direction must:

(a) be in writing; and

(b) specify the reason for the direction.

(4) An entity must comply with a direction given under subsection (2).

Civil penalty: 200 penalty units.

(5) A direction under subsection (2) is not a legislative instrument.

# Division 3—Compliance assessments

## 126 Compliance assessments

(1) The Digital ID Regulator may, by written notice, require an entity to undergo an assessment (a ***compliance assessment***):

(a) for the purposes of determining whether the entity has complied, is complying or is able to comply with this Act; or

(b) if the Digital ID Regulator is satisfied that any of the following has occurred, or is suspected to have occurred, in relation to an accredited entity:

(i) a cyber security incident;

(ii) a digital ID fraud incident;

(iii) a serious or repeated breach of the Accreditation Rules;

(iv) an incident that is having, or may have, a material impact on the operation of the entity's information technology systems through which it provides its accredited services;

(v) an incident that is having, or may have, a material impact on the operation of the Australian Government Digital ID System;

(vi) a change to the entity's operating environment that is having, or may have, a material impact on the entity's risk profile; or

(c) in circumstances specified in the Digital ID Rules.

Note: For variation and revocation of a notice given under this subsection, see subsection 33(3) of the *Acts Interpretation Act 1901*.

(2) The notice must specify:

(a) the period within which the compliance assessment is to be undertaken; and

(b) whether the compliance assessment must be undertaken:

(i) by or on behalf of the Digital ID Regulator; or

(ii) by an independent assessor arranged by the entity.

(3) The entity must comply with the notice within the period specified in the notice.

Note 1: If an entity has applied for approval to participate in the Australian Government Digital ID System and is given a notice under subsection (1), the Digital ID Regulator is not required to make a decision on the application until the assessment is conducted (see subsection 137(4)).

Note 2: For accredited entities and entities that hold an approval to participate in the Australian Government Digital ID System, a failure to comply with a notice given under subsection (1) may lead to compliance action such as suspension and revocation of approvals and accreditation.

(4) The Digital ID Rules may make provision for and in relation to compliance assessments.

(5) Without limiting subsection (4), the Digital ID Rules may make provision for or in relation to the following:

(a) processes to be followed during a compliance assessment or after a compliance assessment has been conducted;

(b) information that must be provided to or by an entity during a compliance assessment or after a compliance assessment has been conducted;

(c) requirements in relation to reports to be provided in relation to a compliance assessment;

(d) actions the Digital ID Regulator may require the entity subject to a compliance assessment to take during the compliance assessment or after the assessment has been conducted.

(6) This section does not limit the Accreditation Rules that may be made for the purposes of section 27.

### 127 Entities must provide assistance to persons undertaking compliance assessments

An entity that is the subject of a compliance assessment must provide the person undertaking the assessment with the facilities and assistance that are reasonably necessary for the conduct of the compliance assessment.

# Division 4—Power to require information or documents

## 128 Power to require information or documents

(1) This section applies if the Digital ID Regulator reasonably believes that an entity has or may have information or documents relevant to:

(a) whether an entity is complying, or has complied, with the entity's obligations under this Act; or

(b) the performance of the Digital ID Regulator's functions, or the exercise of any of the Digital ID Regulator's powers, under this Act.

(2) The Digital ID Regulator may, by written notice, require the entity:

(a) to give to the Digital ID Regulator, within the period and in the manner and form specified in the notice, any such information; or

(b) to produce to the Digital ID Regulator, within the period and in the manner specified in the notice, any such documents.

(3) A period specified in a notice under subsection (2) must not be less than 28 days after the notice is given.

(4) A notice under subsection (2) must contain a statement to the effect that an entity may be liable to a civil penalty if the entity fails to comply with the notice.

(5) An entity must comply with a requirement under subsection (2) within the period and in the manner specified in the notice.

Civil penalty: 200 penalty units.

(6) Subsection (5) does not apply if the entity has a reasonable excuse.

Note: A person who wishes to rely on this subsection bears an evidential burden in relation to the matter mentioned in this subsection (see section 96 of the Regulatory Powers Act).

# Part 3—Record keeping

## 129 Record keeping by participating entities and former participating entities

(1) This section applies to:

(a) entities that hold an approval to participate in the Australian Government Digital ID System; and

(b) entities whose approval to participate in the Australian Government Digital ID System is suspended; and

(c) entities whose approval to participate in the Australian Government Digital ID System has been revoked.

(2) However, this section does not apply to relying parties.

(3) The entity must keep records of the kind, for the period and in the manner prescribed by the Digital ID Rules.

Civil penalty: 200 penalty units.

(4) Digital ID Rules made for the purposes of subsection (3):

(a) must not prescribe records of a kind that do not relate to information obtained by entities through the Australian Government Digital ID System; and

(b) may only prescribe a period of retention of more than 7 years if specified circumstances apply in relation to the record.

Note: For the purposes of paragraph (b), specified circumstances may include legal proceedings involving the entity and the records.

## 130 Destruction or de-identification of certain information

(1) This section applies to:

(a) accredited entities that hold an approval to participate in the Australian Government Digital ID System; and

(b) accredited entities whose approval to participate in the Australian Government Digital ID System is suspended; and

(c) accredited entities whose approval to participate in the Australian Government Digital ID System has been revoked.

(2) The accredited entity must destroy or de-identify information in the possession or control of the entity if:

(a) the information is personal information; and

(b) the information was obtained by the entity through the Australian Government Digital ID System; and

(c) the entity is not required or authorised to retain the information by or under:

(i) this Act; or

(ii) another law of the Commonwealth; or

(iii) a law of a State or Territory; or

(iv) a court/tribunal order (within the meaning of the *Privacy Act 1988*); and

(d) the information does not relate to any current or anticipated legal proceedings or dispute resolution proceedings to which the entity is a party.

Note: For the purposes of subparagraph (c)(i), the entity may be required to retain the information for a specified period under Digital ID Rules made for the purposes of section 129.

Civil penalty: 200 penalty units.

# Part 4—Review of decisions

## 131 Reviewable decisions

(1) A decision by the Digital ID Regulator referred to in column 1 of an item of the following table is a ***reviewable decision***. An entity referred to in column 2 of the item is the ***affected entity*** for the decision.

**Reviewable decisions**

| Item | Column 1<br>*Reviewable decision* | Column 2<br>*Affected entity* |
|---|---|---|
| 1 | A decision under section 15 to refuse to accredit an entity as an accredited entity | The entity who made the application |
| 2 | A decision under subsection 18(2) to impose a condition on an entity's accreditation | The entity on whom the condition is imposed |
| 3 | A decision under subsection 18(2) to refuse to impose, on application by an entity, a condition on the entity's accreditation | The entity who made the application |
| 4 | A decision under subsection 20(1) to vary, on the Digital ID Regulator's own initiative, the conditions imposed on an entity's accreditation | The entity on whom the conditions are imposed |
| 5 | A decision under subsection 20(1) to refuse to vary, on application by an accredited entity, the conditions imposed on the entity's accreditation | The entity who made the application |
| 6 | A decision under subsection 25(2) to suspend the accreditation of an accredited entity | The accredited entity |
| 7 | A decision under subsection 25(5) to refuse to suspend the accreditation | The accredited entity |

Section 131

| **Reviewable decisions** | | |
|---|---|---|
| **Item** | **Column 1**<br>***Reviewable decision*** | **Column 2**<br>***Affected entity*** |
| | of an accredited entity | |
| 8 | A decision under subsection 26(1) to revoke an entity's accreditation | The entity whose accreditation is revoked |
| 9 | A decision under section 59 to refuse to approve an entity to participate in the Australian Government Digital ID System | The entity who made the application |
| 10 | A decision under subsection 60(2) to direct the Digital ID Regulator to suspend an entity's approval to participate in the Australian Government Digital ID System | The entity subject to the direction |
| 11 | A decision under subsection 62(2) to impose a condition on an entity's approval to participate in the Australian Government Digital ID System | The entity on whom the condition is imposed |
| 12 | A decision under subsection 62(2) to refuse to impose, on application by an entity, a condition on the entity's approval to participate in the Australian Government Digital ID System | The entity who made the application |
| 13 | A decision under subsection 64(1) to vary, on the Digital ID Regulator's own initiative, a condition imposed on an entity's approval to participate in the Australian Government Digital ID System | The entity on whom the condition is imposed |
| 14 | A decision under subsection 64(1) to refuse to vary, on application by an entity, a condition imposed on the entity's approval to participate in the Australian Government Digital ID System | The entity who made the application |

| **Reviewable decisions** | | |
|---|---|---|
| **Item** | **Column 1**<br>***Reviewable decision*** | **Column 2**<br>***Affected entity*** |
| 15 | A decision under subsection 69(2) to suspend an entity's approval to participate in the Australian Government Digital ID System | The entity that holds the approval |
| 16 | A decision under subsection 69(5) to refuse to suspend, on application by an entity, the entity's approval to participate in the Australian Government Digital ID System | The entity who made the application |
| 17 | A decision under subsection 69(12) to refuse to revoke a suspension of an entity's approval to participate in the Australian Government Digital ID System | The entity whose approval is suspended |
| 18 | A decision under subsection 70(1) to revoke an entity's approval to participate in the Australian Government Digital ID System | The entity that held the approval |
| 19 | A decision under subsection 71(3) to refuse to grant an exemption to a participating relying party | The participating relying party who made the application |
| 20 | A decision under subsection 81(1) to direct an accredited entity to maintain adequate insurance | The entity subject to the direction |
| 21 | A decision to give a direction to an entity under Division 2 of Part 2 of Chapter 8 | The entity subject to the direction |

(2) The Digital ID Rules may also:

(a) provide that a decision made under a specified provision of this Act is a ***reviewable decision***; and

(b) specify the entity who is an ***affected entity*** for the reviewable decision.

(3) If, under subsection (2):

(a) the Digital ID Rules provide that a decision made under the Digital ID Rules is a reviewable decision; and

(b) the person making the decision is not the Digital ID Regulator (or a delegate of the Digital ID Regulator);

sections 132, 133 and 134 have effect as if a references in those sections to the Digital ID Regulator were references to the person making the decision.

(4) Despite subsection (1), a decision made for reasons of security (within the meaning of the *Australian Security Intelligence Organisation Act 1979*) in relation to an entity that is not an Australian entity is not a ***reviewable decision***.

## 132 Internal review of decisions made by delegates of the Digital ID Regulator

(1) If an entity is affected by a reviewable decision made by a delegate of the Digital ID Regulator, the entity may apply in writing to the Digital ID Regulator for review (the ***internal review***) of the decision.

(2) An application for internal review must be made within 28 days after the day on which the decision first came to the notice of the applicant.

## 133 Reconsideration by Digital ID Regulator

(1) Within 90 days after receiving an application under section 132 for internal review, the Digital ID Regulator must:

(a) review the decision; and

(b) affirm, vary or revoke the decision; and

(c) if the Digital ID Regulator revokes the decision—make such other decision (if any) that the Digital ID Regulator thinks appropriate.

(2) The Digital ID Regulator must, as soon as practicable after making a decision under subsection (1), give the applicant a written statement of the Digital ID Regulator's reasons for the decision.

(3) If the Digital ID Regulator's functions under this section are performed by a delegate of the Digital ID Regulator, the delegate who makes the decision under subsection (1):

(a) must not have been involved in making the original reviewable decision; and

(b) must hold a position or perform duties of a higher level than the delegate who made the original reviewable decision.

### 134 Review by the Administrative Appeals Tribunal

(1) Applications may be made to the Administrative Appeals Tribunal for review of the following decisions:

(a) a reviewable decision made by the Digital ID Regulator personally;

(b) an internal review decision made by the Digital ID Regulator under subsection 133(1).

(2) An application under subsection (1) may be made only by, or on behalf of, an affected entity for the reviewable decision.

(3) Subsection (2) has effect despite subsection 27(1) of the *Administrative Appeals Tribunal Act 1975*.

# Part 5—Applications under this Act

## 135 Requirements for applications

(1) An application made under this Act must:

(a) be given in a form and manner for that kind of application approved by the person to whom the application is made; and

(b) be accompanied by any information or documents required by the form; and

(c) be accompanied by any information or documents required by the Digital ID Rules or the Accreditation Rules; and

(d) if Digital ID Rules made for the purposes of section 138 specify a fee that must accompany the application and payment of the fee has not been waived—be accompanied by the fee.

Note: A decision on an application is not required to be made if this subsection is not complied with (see section 137).

(2) The person to whom the application is made may accept any information or document previously given to the person in connection with another application made under this Act as satisfying any requirement to give that information or document under subsection (1).

(3) To avoid doubt, approval may be given for:

(a) different forms for different kinds of applications; or

(b) a single form for more than one kind of application.

## 136 Powers in relation to applications

(1) If a person (the ***applicant***) makes an application under this Act, the person to whom the application is made may, by written notice, require the applicant to give the person such further information or documents in relation to the application as the person reasonably requires.

Note 1: The person is not required to make a decision on the application if this subsection is not complied with (see section 137).

Note 2: The Digital ID Regulator may also require an applicant to undergo a compliance assessment before making a decision on the application (see section 126).

(2) A notice under subsection (1) may specify a period, which must not be less than 14 days, within which the information or documents must be given.

### 137 Decisions not required to be made in certain circumstances

(1) If this Act requires an application to be in a form approved by the person to whom the application is made, the person is not required to make a decision on the application if it is not in that form.

(2) If this Act requires an application to be accompanied by information or documents, the person to whom the application is made is not required to make a decision on the application until the information or documents are provided.

(3) If this Act permits a person to require further information or documents in relation to an application, the person is not required to make a decision on the application until the information or documents are provided.

(4) If the Digital ID Regulator requires a compliance assessment to be conducted for the purposes of making a decision under this Act, the Digital ID Regulator is not required to make the decision until the assessment is conducted.

(5) If Digital ID Rules made for the purposes of section 138 specify a fee that must accompany an application and payment of the fee has not been waived, the person to whom the application is made is not required to make a decision on the application until the fee is paid.

# Part 6—Fees

## Division 1—Fees charged by the Digital ID Regulator

### 138 Charging of fees by Digital ID Regulator etc.

(1) The Digital ID Rules may make provision in relation to the charging of fees by:

(a) the Digital ID Regulator for activities carried out by or on behalf of the Digital ID Regulator in performing functions or exercising powers under this Act; or

(b) other persons to whom application may be made under this Act.

(2) Without limiting subsection (1), the Digital ID Rules may do any of the following:

(a) prescribe a fee by specifying the amount of the fee or a method of working out the fee;

(b) specify that the amount of a fee is the cost incurred by the Digital ID Regulator in arranging and paying for another person to carry out a relevant activity;

(c) make provision for when and how fees are to be paid;

(d) make provision in relation to penalties for late payment of specified fees;

(e) make provision in relation to the refund, remission or waiver of specified fees or penalties for late payment of specified fees.

(3) However, the Digital ID Rules made for the purposes of subsection (1) must not provide for the charging of a fee to an individual for the creation or use of a digital ID of the individual.

(4) A fee prescribed by the Digital ID Rules made under subsection (1) is payable to the Commonwealth.

(5) The amount of a fee may be nil.

(6) A fee prescribed by the Digital ID Rules must not be such as to amount to taxation.

(7) If a fee is payable for a service, the service need not be provided while the fee remains unpaid. The Digital ID Rules may provide for the extension of any times for providing services accordingly.

### 139 Review of fees

(1) The Minister must cause periodic reviews of rules made for the purposes of subsection 138(1) to be undertaken.

(2) The first review must:

(a) start no later than 2 years after rules made for the purposes of the relevant subsection commence; and

(b) be completed within 12 months.

(3) Subsequent reviews must:

(a) start no later than every 2 years after the completion of the previous review; and

(b) be completed within 12 months.

(4) The Minister must cause a written report about each review to be prepared and published on the Digital ID Regulator's website.

### 140 Recovery of fees charged by the Digital ID Regulator

A fee charged by the Digital ID Regulator that is due and payable to the Commonwealth under this Act may be recovered as a debt due to the Commonwealth by action in a court of competent jurisdiction.

### 141 Commonwealth not liable to pay fees charged by entities that are part of the Commonwealth

(1) The Commonwealth is not liable to pay a fee that is payable under this Act to a part of the Commonwealth that is not a separate legal entity. However, it is the Parliament's intention that the Commonwealth should be notionally liable to pay such a fee.

(2) The Finance Minister may give such written directions as are necessary or convenient for carrying out or giving effect to subsection (1) and, in particular, may give directions in relation to the transfer of money within an account, or between accounts, operated by the Commonwealth.

(3) Directions under subsection (2) have effect, and must be complied with, despite any other law of the Commonwealth.

(4) Directions under subsection (2) are not legislative instruments.

(5) In this subsection:

***Commonwealth*** includes a Commonwealth entity (within the meaning of the *Public Governance, Performance and Accountability Act 2013)* that cannot be made liable to taxation by a law of the Commonwealth.

## Division 2—Fees charged by accredited entities

### 142 Charging of fees by accredited entities in relation to the Australian Government Digital ID System

(1) An accredited entity that charges fees in relation to its accredited services that it provides in relation to the Australian Government Digital ID System must do so in accordance with the Digital ID Rules (if any) made for the purposes of subsection (2).

(2) The Digital ID Rules may make provision in relation to the charging of fees by accredited entities for services provided in relation to Australian Government Digital ID System.

(3) Without limiting subsection (2), the Digital ID Rules may do any of the following:

(a) prescribe a fee by specifying the amount of the fee or a method of working out the fee;

(b) make provision for when and how fees may be charged;

(c) make provision in relation to the conduct of periodic reviews of fees;

(d) make provision for any other matters in relation to the charging of fees, including in relation to exemptions, refunds, remissions or waivers.

(4) The amount of a fee may be nil.

(5) This section, and rules made for the purposes of subsection (2), do not otherwise affect the ability of an accredited entity to charge fees for its accredited services, either in relation to the Australian Government Digital ID System or otherwise.

# Chapter 9—Other matters

## 143 Simplified outline of this Chapter

## 144 Annual report by Digital ID Regulator

(1) After the end of each financial year, the Digital ID Regulator must prepare and give a report to the Minister, for presentation to the Parliament, on the Digital ID Regulator's activities during the financial year.

(2) The report must include the following:

(a) information about the operation of the accreditation scheme, including:

(i) the number of applications for accreditation made under section 14; and

(ii) the number of accreditations granted under section 15;

(b) information about the operation of the Australian Government Digital ID System, including:

(i) the number of applications made to participate in the system under section 58; and

(ii) the number of approvals granted to participate in the system under section 59; and

(iii) the number of digital ID fraud incidents or cyber security incidents, and the responses to any such incidents;

(c) information on any other matters notified by the Minister to the Digital ID Regulator.

(3) The report must be given to the Minister by:

(a) the 30th day of October; or

(b) the end of any further period granted under subsection 34C(5) of the *Acts Interpretation Act 1901*.

### 145 Annual report by Information Commissioner

The annual report prepared by the Information Commissioner and given to the Minister under section 46 of the *Public Governance, Performance and Accountability Act 2013* for a period must include information about the performance of the Information Commissioner's functions, and the exercise of the Information Commissioner's powers, under or in relation to Part 2 of Chapter 3 of this Act during the period.

### 146 Treatment of partnerships

(1) This Act applies to a partnership as if it were a person, but with the changes set out in this section.

(2) An obligation that would otherwise be imposed on the partnership by this Act is imposed on each partner instead, but may be discharged by any of the partners.

(3) A civil penalty provision of this Act that would otherwise have been contravened by the partnership is taken to have been contravened by each partner in the partnership, at the time the provision was contravened, who:

(a) did the relevant act or made the relevant omission; or

(b) aided, abetted, counselled or procured the relevant act or omission; or

(c) was in any way knowingly concerned in, or party to, the relevant act or omission (whether directly or indirectly and whether by any act or omission of the partner).

(4) For the purposes of this Act, a change in the composition of a partnership does not affect the continuity of the partnership.

### 147 Treatment of unincorporated associations

(1) This Act applies to an unincorporated association as if it were a person, but with the changes set out in this section.

(2) An obligation that would otherwise be imposed on the association by this Act is imposed on each member of the association's

committee of management instead, but may be discharged by any of the members.

(3) A civil penalty provision of this Act that would otherwise have been contravened by the unincorporated association is taken to have been contravened by each member of the committee of management of the association at the time the provision was contravened, who:

(a) did the relevant act or made the relevant omission; or

(b) aided, abetted, counselled or procured the relevant act or omission; or

(c) was in any way knowingly concerned in, or party to, the relevant act or omission (whether directly or indirectly and whether by any act or omission of the member).

## 148 Treatment of trusts

(1) This Act applies to a trust as if it were a person, but with the changes set out in this section.

(2) If a trust has a single trustee:

(a) an obligation that would otherwise be imposed on the trust by this Act is imposed on the trustee instead; and

(b) a civil penalty provision of this Act that would otherwise have been contravened by the trust is taken to have been contravened by the trustee.

(3) If a trust has 2 or more trustees:

(a) an obligation that would otherwise be imposed on the trust by this Act is imposed on each trustee instead, but may be discharged by any of the trustees; and

(b) a civil penalty provision of this Act that would otherwise have been contravened by the relevant entity is taken to have been contravened by each trustee of the relevant entity, at the time the provision was contravened, who:

(i) did the relevant act or made the relevant omission; or

(ii) aided, abetted, counselled or procured the relevant act or omission; or

(iii) was in any way knowingly concerned in, or party to, the relevant act or omission (whether directly or indirectly and whether by any act or omission of the trustee).

## 149 Treatment of certain Commonwealth, State and Territory entities

*Government entities*

(1) This Act applies to any of the following entities (***government entities***) as if it were a person (if it is otherwise not a person), but with the changes set out in this section:

(a) a Commonwealth entity (within the meaning of the *Public Governance, Performance and Accountability Act 2013*);

(b) a person or body that is an agency within the meaning of the *Freedom of Information Act 1982*;

(c) a body specified, or the person holding an office specified, in Part I of Schedule 2 to the *Freedom of Information Act 1982*;

(d) a department or authority of a State;

(e) a department or authority of a Territory.

*Persons who may engage in conduct on behalf of government entities*

(2) If this Act authorises or requires a government entity to engage in conduct, the conduct may be engaged in on behalf of the government entity by a relevant person for the entity, if engaging in the conduct is within the scope of the relevant person's employment or authority.

*Determining how government entities breach this Act*

(3) In determining whether a government entity has breached this Act:

(a) conduct engaged in on behalf of the entity by a relevant person for the entity acting within the scope (actual or apparent) of the relevant person's employment or authority is taken to have been engaged in instead by the entity; and

(b) if it is necessary to establish intention, knowledge or recklessness, or any other state of mind, of the entity, it is sufficient to establish the intention, knowledge or recklessness, or other state of mind, of the person mentioned in paragraph (a).

(4) Despite paragraph (3)(a), a government entity does not contravene a civil penalty provision of this Act because of conduct of a person that the entity is taken to have engaged in, if it is established that the entity took reasonable precautions and exercised due diligence to avoid the conduct.

*Infringement notices may be given to government entities*

(5) If an infringement notice is to be given to the Commonwealth, a State or a Territory under Part 5 of the Regulatory Powers Act, the government entity whose acts or omissions are alleged to have contravened the provision subject to the infringement notice may be specified in the infringement notice.

*Civil penalty proceedings and government entities*

(6) If civil penalty proceedings are brought against the Commonwealth, a State or a Territory in relation to a contravention of a civil penalty provision of this Act, the government entity whose acts or omissions are alleged to have contravened the provision may be specified in any document initiating, or relating to, the proceedings.

(7) Despite paragraph 82(5)(b) of the Regulatory Powers Act, if a government entity contravenes a civil penalty provision of this Act, the maximum penalty that a court may order the entity to pay is 5 times the pecuniary penalty specified for the civil penalty provision.

*Relevant person*

(8) In this section:

***relevant person*** for an entity means:

(a) the head (however described) of the entity; or
(b) a statutory officeholder of the entity; or
(c) an officer, employee or member of the entity; or
(d) a person that is party to a contract with the entity; or
(e) an agent of the entity.

### 150 Bodies corporate and due diligence

For the purposes of section 97 of the Regulatory Powers Act (about attributing contraventions of employees etc. to a body corporate), a body corporate does not contravene a civil penalty provision of this Act because of conduct of a person that the body corporate is taken to have engaged in, if it is established that the body corporate took reasonable precautions and exercised due diligence to avoid the conduct.

### 151 Protection from civil action

(1) This section applies to the following:
(a) the Digital ID Regulator;
(b) a member of the Commission (within the meaning of the *Competition and Consumer Act 2010*);
(c) an associate member of the Australian Competition and Consumer Commission;
(d) a member of the staff of the Australian Competition and Consumer Commission.

(2) A person mentioned in subsection (1) is not liable to an action or other proceeding for damages for, or in relation to, an act done or omitted to be done in good faith by the person:
(a) in the performance, or purported performance, of any functions under this Act; or
(b) in the exercise, or purported exercise, of any powers under this Act.

## 152 Geographical jurisdiction of civil penalty provisions

*Geographical jurisdiction of civil penalty provisions*

(1) An entity does not contravene a civil penalty provision of this Act unless:

(a) the conduct constituting the alleged contravention occurs wholly or partly in Australia, or wholly or partly on board an Australian aircraft or Australian ship; or

(b) the conduct constituting the alleged contravention occurs wholly outside Australia and a result of the conduct occurs:

(i) wholly or partly in Australia; or

(ii) wholly or partly on board an Australian aircraft or an Australian ship; or

(c) the conduct constituting the alleged contravention occurs wholly outside Australia and, at the time of the alleged contravention, the entity is an Australian entity; or

(d) all of the following conditions are satisfied:

(i) the alleged contravention is an ancillary contravention;

(ii) the conduct constituting the alleged contravention occurs wholly outside Australia;

(iii) the conduct constituting the primary contravention to which the ancillary contravention relates, or a result of that conduct, occurs wholly or partly in Australia or wholly or partly on board an Australian aircraft or an Australian ship.

*Defence for primary contravention*

(2) Despite subsection (1), an entity does not contravene a civil penalty provision of this Act if:

(a) the alleged contravention is a primary contravention; and

(b) the conduct constituting the alleged contravention occurs wholly in a foreign country, but not on board an Australian aircraft or Australian ship; and

(c) the entity is not an Australian entity; and

(d) there is not in force, in the foreign country or the part of the foreign country where the conduct constituting the alleged contravention or offence occurred, a law creating a pecuniary or criminal penalty for conduct corresponding to the conduct constituting the alleged contravention.

*Defence for ancillary contravention*

(3) Despite subsection (1), an entity does not contravene a civil penalty provision of this Act if:

(a) the alleged contravention is an ancillary contravention; and

(b) the conduct constituting the alleged contravention occurs wholly in a foreign country, but not on board an Australian aircraft or an Australian ship; and

(c) the conduct constituting the primary contravention to which the alleged contravention relates, or a result of that conduct, occurs wholly in a foreign country, but not on board an Australian aircraft or Australian ship; and

(d) the entity is not an Australian entity; and

(e) there is not in force, in the foreign country or the part of the foreign country where the conduct constituting the alleged contravention occurred, a law creating a pecuniary or criminal penalty for conduct corresponding to the conduct constituting the primary contravention to which the alleged contravention relates.

*Evidential burden*

(4) An entity who is alleged to have contravened a civil penalty provision of this Act and who wishes to rely on subsection (2) or (3) bears an evidential burden (within the meaning of the Regulatory Powers Act) in relation to the matters set out in the subsection.

*Other matters*

(5) A reference in this section to a result of conduct is a reference to a result that is an element of the civil penalty provision.

(6) For the purposes of this section and without limitation, if an entity sends, or causes to be sent, an electronic communication or other thing:

(a) from a point outside Australia to a point in Australia; or

(b) from a point in Australia to a point outside Australia;

that conduct is taken to have occurred partly in Australia.

*Definitions*

(7) In this section:

***ancillary contravention*** of a civil penalty provision means a contravention that arises out of the operation of section 92 of the Regulatory Powers Act.

***Australian aircraft*** has the same meaning as in the *Criminal Code*.

***Australian ship*** has the same meaning as in the *Criminal Code*.

***electronic communication*** has the same meaning as in the *Criminal Code*.

***foreign country*** has the same meaning as in the Criminal Code.

***point*** includes a mobile or potentially mobile point, whether on land, underground, in the atmosphere, underwater, at sea or anywhere else.

***primary contravention*** of a civil penalty provision means a contravention that does not arise out of the operation of section 92 of the Regulatory Powers Act.

## 153 Review of operation of Act

(1) The Minister must cause a review of the operation of this Act to be undertaken.

(2) The review must be undertaken no later than 2 years after the commencement of this Act.

(3) The persons who undertake the review must give the Minister a written report of the review.

(4) The Minister must cause a copy of the report to be tabled in each House of the Parliament within 15 sitting days of that House after the Minister receives the report.

## 154 Delegation—Minister

(1) The Minister may, in writing, delegate all or any of the Minister's functions or powers under this Act (other than the Minister's power under section 158) to any of the following:

(a) the Digital ID Regulator;

(b) the Secretary;

(c) an SES employee or acting SES employee in the Department.

Note: Sections 34AA to 34A of the *Acts Interpretation Act 1901* contain provisions relating to delegations.

(2) In exercising powers or performing functions under the delegation, the delegate must comply with any written directions of the Minister.

## 155 Delegation—Digital ID Regulator

The Digital ID Regulator may, by resolution, delegate all or any of the Digital ID Regulator's powers or functions under this Act to:

(a) member of the Commission (within the meaning of the *Competition and Consumer Act 2010*); or

(b) an SES employee, or an acting SES employee, in the Australian Competition and Consumer Commission; or

(c) an SES employee, or an acting SES employee, in the Department.

Note 1: The Digital ID Regulator is the Australian Competition and Consumer Commission (see section 85).

Note 2: Sections 34AA to 34A of the *Acts Interpretation Act 1901* contain provisions relating to delegations.

### 156 Delegation—Digital ID Data Standards Chair

(1) The Digital ID Data Standards Chair may delegate, in writing, any or all of the Chair's functions or powers to a person assisting the Chair under section 110 who is:

(a) an SES employee, or an acting SES employee; or

(b) an APS employee who is holding or performing the duties of a specified office or position that the Chair is satisfied is sufficiently senior for the APS employee to perform the function or exercise the power.

(2) Subsection (1) does not apply to the function referred to in paragraph 93 (about making standards).

(3) In performing a delegated function or exercising a delegated power, the delegate under subsection (1) must comply with any directions of the Digital ID Data Standards Chair.

### 157 Instruments may incorporate etc. material as in force or existing from time to time

(1) This section applies to the following instruments (each of which is a ***core instrument***):

(a) the Accreditation Rules;

(b) the Digital ID Data Standards;

(c) the Digital ID Rules.

(2) A core instrument may make provision in relation to a matter by applying, adopting or incorporating, with or without modification, any matter contained in any other instrument or other writing (an ***incorporated instrument***) as in force or existing from time to time.

(3) If a core instrument makes provision in relation to a matter in accordance with subsection (2), the core instrument may also make provision in relation to when changes to an incorporated instrument take effect for the purposes of the core instrument.

(4) Subsection (2) has effect despite subsection 14(2) of the *Legislation Act 2003*.

### 158 Rules—general matters

(1) The Minister may, by legislative instrument, make rules prescribing matters:

(a) required or permitted by this Act to be prescribed by the rules; or

(b) necessary or convenient to be prescribed for carrying out or giving effect to this Act.

(2) Without limiting subsection 33(3A) of the *Acts Interpretation Act 1901*, the rules may prescribe a matter or thing differently for different kinds of entities, things or circumstances.

(3) The rules may make provision for or in relation to a matter by conferring a power on the Digital ID Regulator or the Minister to:

(a) make an instrument of an administrative character; or

(b) make a decision of an administrative character.

(4) To avoid doubt, the rules may not do the following:

(a) create an offence or civil penalty;

(b) provide powers of:

(i) arrest or detention; or

(ii) entry, search or seizure;

(c) impose a tax;

(d) set an amount to be appropriated from the Consolidated Revenue Fund under an appropriation in this Act;

(e) directly amend the text of this Act.

(5) In this section, a reference to this Act does not include a reference to:

(a) the Accreditation Rules; or

(b) the Digital ID Rules.

### 159 Rules—requirement to consult

*General requirement to consult*

(1) Before making or amending any rules under section 158, the Minister must:

(a) cause to be published on the Department's website a notice:

(i) setting out the draft rules or amendments; and

(ii) inviting persons to make submissions to the Minister about the draft rules or amendments within the period specified in the notice (which must be at least 28 days after the notice is published); and

(b) if the rules deal with matters that relate to the privacy functions (within the meaning of the *Australian Information Commissioner Act 2010*)—consult the Information Commissioner; and

(c) consider any submissions received within the specified period.

(2) Without paragraph (1)(b), the Minister must consult the Information Commissioner if the rules will provide that accredited entities, or specified kinds of accredited entities, are authorised to:

(a) collect or disclose restricted attributes of individuals; or

(b) collect, use or disclose biometric information of individuals.

(3) The Minister may consider any submissions received after the specified period if the Minister considers it appropriate to do so.

*Exception if imminent threat etc.*

(4) Subsection (1) does not apply if:

(a) the Minister is satisfied that there is an imminent threat to the Australian Government Digital ID System; or

(b) the Minister is satisfied that a hazard has had, or is having, a significant impact on the Australian Government Digital ID System.

*Review*

(5) If:

(a) because of subsection (4), subsection (1) did not apply to the making of rules or amendments; and

(b) the rules or amendments have not been disallowed by either House of the Parliament;

the Secretary must:

(c) review the operation, effectiveness and implications of the rules or amendments; and

(d) without limiting paragraph (a), consider whether any amendments should be made; and

(e) give the Minister a report of the review and a statement setting out the Secretary's findings.

(6) For the purposes of the review, the Secretary must:

(a) cause to be published on the Department's website a notice:

(i) setting out the rules or amendments concerned; and

(ii) inviting persons to make submissions to the Secretary about the rules or amendments concerned within the period specified in the notice (which must be at least 28 days after the notice is published); and

(b) if the rules deal with matters that relate to the privacy functions (within the meaning of the *Australian Information Commissioner Act 2010*)—consult the Information Commissioner; and

(c) consider any submissions received within the specified period.

*Findings of review to be tabled*

(7) The Secretary must complete the review within 60 days after the commencement of the rules or amendments concerned.

(8) The Minister must cause a copy of the statement of findings to be tabled in each House of the Parliament within 15 sitting days of that House after the Minister receives it.

*Failure to comply does not affect validity etc.*

(9) A failure to comply with this section does not affect the validity or enforceability of any rules, or any amendments to any rules.

*Relationship with the Legislation Act 2003*

(10) This section does not limit section 17 of the *Legislation Act 2003* (rule-makers should consult before making legislative instrument).