2019-2020-2021

The Parliament of the
Commonwealth of Australia

HOUSE OF REPRESENTATIVES

EXPOSURE DRAFT

Trusted Digital Identity Bill 2021

No. , 2021

(Prime Minister)

A Bill for an Act to establish the trusted digital identity system and to provide for the accreditation of entities in relation to digital identity systems generally, and for related purposes

Contents

Chapter 1—Introduction 2

Part 1—Preliminary 2

1 Short title 2
2 Commencement 2
3 Objects 3
4 Simplified outline of this Act 4
5 Act binds the Crown 4
6 Extension to external Territories 4
7 Extraterritorial operation 4
8 Concurrent operation of State and Territory laws 4

Part 2—Interpretation 5

9 Definitions 5
10 Meaning of *attribute* of an individual 11
11 Meaning of *restricted attribute* of an individual 12
12 Fit and proper person considerations 13

Chapter 2—The trusted digital identity system 14

Part 1—Introduction 14

13 Simplified outline of this Chapter 14

Part 2—The trusted digital identity system 15

Division 1—The trusted digital identity system 15

14 Oversight Authority may develop, operate and maintain the trusted digital identity system 15
15 Circumstances in which entities may onboard to the trusted digital identity system 15

Division 2—Onboarding to the trusted digital identity system 19

16 Applying for approval to onboard to the trusted digital identity system 19
17 Applicants may be required to enter into trusted provider agreements 19
18 Approval to onboard to the trusted digital identity system 19
19 Entities may be taken to be approved to onboard to the trusted digital identity system 21
20 Minister's directions regarding onboarding 21

21 Approval to onboard to the trusted digital identity system is subject to conditions 22
22 Conditions on approval to onboard to the trusted digital identity system 23
23 Conditions relating to restricted attributes of individuals 25
24 Variation and revocation of conditions 27
25 Notice before changes to conditions on approval 27
26 Notice of decision of changes of conditions on approval 28
27 Applying for variation or revocation of conditions on approval 29

Division 3—Suspension and revocation of approval to onboard 30
28 Suspension of approval to onboard to the trusted digital identity system 30
29 Revocation of approval to onboard to the trusted digital identity system 32

Division 4—Other matters relating to the trusted digital identity system 35
30 Generating and using a digital identity is voluntary 35
31 Holding etc. digital identity information outside Australia 36
32 Reportable incidents 37
33 Interoperability obligation 38
34 Exemption from interoperability obligation 40
35 Trusted provider agreements 40
36 Technical standards 41
37 Entities may conduct testing in relation to the trusted digital identity system 42
38 Use and disclosure of personal information to conduct testing 42

Part 3—Liability and redress framework 43

Division 1—Liability of onboarded entities 43
39 Accredited entities onboarded to the system protected from liability in certain circumstances 43

Division 2—Statutory contact 44
40 Statutory contract between entities onboarded to the system 44
41 Onboarded entities to maintain insurance as directed by Oversight Authority 45
42 Dispute resolution procedures 45

Division 3—Redress framework 46
43 Redress obligations of accredited entities 46

44 Redress obligations of participating relying parties 47
45 TDI rules may prescribe redress obligations 48
46 Oversight Authority to assist individuals and businesses affected by incidents 48

Chapter 3—Accreditation 50

Part 1—Introduction 50
47 Simplified outline of this Chapter 50

Part 2—Accreditation 51

Division 1—Applying for accreditation 51
48 Authorisation to apply for accreditation 51
49 Applications for accreditation 51

Division 2—Accreditation 53
50 Oversight Authority must decide whether to accredit an entity 53
51 Accreditation is subject to conditions 54
52 Conditions of accreditation 55
53 Variation and revocation of conditions of accreditation 56
54 Notice before changes to conditions on accreditation 56
55 Notice of decision of changes to conditions on accreditation 57
56 Applying for variation or revocation of conditions on accreditation 57

Division 3—Suspension and revocation of accreditation 58
57 Suspension of accreditation 58
58 Revocation of accreditation 60

Division 4—TDIF accreditation rules 62
59 TDIF accreditation rules 62
60 TDIF accreditation rules may incorporate etc. material as in force or existing from time to time 63

Division 5—Other matters relating to accredited entities 64
61 Digital identities must be deactivated on request 64
62 Services provided by accredited entities must be accessible and inclusive 64

Chapter 4—Privacy 65

Part 1—Introduction 65
63 Simplified outline of this Chapter 65

Part 2—Privacy 66

Division 1—Interaction with the Privacy Act 1988 66

64 Extended meaning of *personal information* 66
65 Privacy obligations for non-APP entities 66
66 Contraventions of Division 2 are interferences with privacy 67
67 Notification of eligible data breaches—accredited entities that are APP entities 68
68 Notification of eligible data breaches—accredited entities (other than State or Territory bodies) that are not APP entities 68
69 Notification of corresponding data breaches—accredited State or Territory entities that are not APP entities 69
70 Additional function of the Information Commissioner 70
71 Information Commissioner may disclose details of investigations to Oversight Authority 70
72 Commissioner may share information with State or Territory privacy authorities 71

Division 2—Additional privacy safeguards 72

73 Individuals must expressly consent to disclosure of attributes of individuals to relying parties 72
74 Disclosure of restricted attributes of individuals 72
75 Prohibition on single identifiers 73
76 Restrictions on collecting, using and disclosing biometric information 74
77 Authorised collection, use and disclosure of biometric information of an individual—general rules 74
78 Government entities collecting etc. biometric information for other purposes 76
79 Deletion of biometric information of individuals 77
80 Prohibition on data profiling 78
81 Digital identity information must not be used for prohibited enforcement purposes 79
82 Digital identity information must not be used or disclosed for prohibited marketing purposes 80
83 Accredited identity exchanges must not retain attributes or restricted attributes of individuals 81

Chapter 5—TDIF trustmarks 82

84 TDIF trustmarks 82
85 Authorised use of TDIF trustmarks etc. 82

Chapter 6—Oversight Authority 84

Part 1—Oversight Authority 84

Division 1—Establishment and functions of the Oversight Authority 84

86 Oversight Authority 84
87 Functions of the Oversight Authority 84
88 Powers of the Oversight Authority 85
89 Independence of Oversight Authority 85

Division 2—Appointment of the Oversight Authority 86

90 Appointment 86
91 Term of appointment 86
92 Acting Oversight Authority 86
93 Application of the finance law 86

Division 3—Terms and conditions for the Oversight Authority 87

94 Remuneration 87
95 Leave of absence 87
96 Outside work 87
97 Disclosure of interests 88
98 Resignation of appointment 88
99 Suspension or termination of appointment 88

Division 4—Staff assisting the Oversight Authority 90

100 Staff 90
101 Consultants 90
102 Contractors 90

Division 5—Protecting personal and commercially sensitive information 91

103 Prohibition on Oversight Authority and staff using or disclosing personal or commercially sensitive information 91
104 Authorised uses and disclosures of personal or commercially sensitive information 92
105 Disclosing personal or commercially sensitive information to courts and tribunals etc. 93

Part 2—Advisory boards and committees 94

106 Establishment and functions of trusted digital identity advisory board 94
107 Trusted digital identity advisory board members 94

108 Trusted digital identity advisory board members—remuneration....95
109 Trusted digital identity advisory board members—leave of absence....95
110 Outside employment....95
111 Trusted digital identity advisory board members—disclosure of interests....95
112 Trusted digital identity advisory board members—resignation and termination....96
113 Trusted digital identity advisory board members—other terms and conditions....97
114 Trusted digital identity advisory board procedures....97
115 Advisory committees....97

Chapter 7—Administration 99

Part 1—Introduction 99

116 Simplified outline of this Chapter....99

Part 2—Registers 100

117 TDIF accredited entities register....100
118 TDIS register....101

Part 3—Compliance and enforcement 104

Division 1—Powers of investigation and enforcement 104

119 Civil penalty provisions....104
120 Infringement notices....105
121 Enforceable undertakings....105
122 Injunctions....106

Division 2—Directions powers 108

123 Oversight Authority's power to give directions to entities in relation to onboarding and accreditation....108
124 Oversight Authority's power to give directions to protect the integrity or performance of the trusted digital identity system....109
125 Remedial directions to accredited entities etc....110

Division 3—Compliance assessments 111

126 Compliance assessments....111
127 Entities must provide assistance to persons undertaking compliance assessments....112
128 Approved assessors....113
129 Approved assessors may charge fees....113

Division 4—Power to require information or documents 114
130 Power to require information or documents 114

Part 4—Record keeping 115
131 Record keeping by onboarded entities and former onboarded entities 115
132 Destruction or de-identification of certain information 115

Part 5—Review of decisions 117
133 Reviewable decisions 117
134 Internal review—decisions made by delegates of the Oversight Authority 120
135 Reconsideration by Oversight Authority 120
136 Review by the Administrative Appeals Tribunal 121

Part 6—Applications under this Act 122
137 Requirements for applications 122
138 Powers of Oversight Authority in relation to applications 122
139 Oversight Authority not required to make a decision in certain circumstances 123

Part 7—Fees 124

Division 1—Fees charged by the Oversight Authority 124
140 Charging of fees by Oversight Authority 124
141 Review of fees 125
142 Recovery of fees charged by the Oversight Authority 125
143 Commonwealth not liable to pay fees charged by the Oversight Authority 125

Division 2—Fees charged by accredited entities 127
144 Charging of fees by accredited entities in relation to the trusted digital identity system 127

Chapter 8—Other matters 128
145 Simplified outline of this Chapter 128
146 Annual report by Oversight Authority 128
147 Annual report by Information Commissioner 129
148 Treatment of partnerships 129
149 Treatment of unincorporated associations 129
150 Treatment of trusts 130
151 Treatment of certain Commonwealth, State and Territory entities 131

152	Protection from civil action	133
153	Geographical jurisdiction of civil penalty provisions	133
154	Review of operation of Act	136
155	Delegation—Minister	136
156	Delegation—Oversight Authority	136
157	Rules—general matters	137
158	Rules—requirement to consult	138

A Bill for an Act to establish the trusted digital identity system and to provide for the accreditation of entities in relation to digital identity systems generally, and for related purposes

The Parliament of Australia enacts:

Chapter 1—Introduction

Part 1—Preliminary

1 Short title

This Act is the *Trusted Digital Identity Act 2021*.

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. 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 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 identity services;

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

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

(2) These objects are to be achieved by:

(a) establishing a trusted digital identity system that is safe, secure, trusted, accessible, easy to use, reliable and voluntary, and supported by strong privacy and integrity safeguards; and

(b) facilitating choice for individuals amongst providers of services within the trusted digital identity system; and

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

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

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

Section 4

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, and the Regulatory Powers Act as it applies in relation to this Act, extend to every external Territory.

7 Extraterritorial operation

(1) This Act, and the Regulatory Powers Act as it applies in relation to this Act, extend to acts, omissions, matters and things outside Australia.

Note: Geographical jurisdiction for civil penalty provisions is dealt with in section 153.

(2) This Act, and the Regulatory Powers Act as it applies in relation to this Act, have 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:

accredited attribute service provider means an attribute service provider that is accredited under section 50 as an accredited attribute service provider.

accredited credential service provider means a credential service provider that is accredited under section 50 as an accredited credential service provider.

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

(a) an accredited attribute service provider;

(b) an accredited credential service provider;

(c) an accredited identity exchange;

(d) an accredited identity service provider;

(e) if rules made for the purposes of paragraph 49(1)(e) prescribe an entity—an entity that is accredited as that kind of entity.

accredited facility of an entity means the facility through which the entity provides the services for which the entity is accredited.

accredited identity exchange means an identity exchange that is accredited under section 50 as an accredited identity exchange.

accredited identity service provider means an identity service provider that is accredited under section 50 as an accredited identity service provider.

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 133.

Section 9

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

approved assessor means a person approved under subsection 128(1).

attribute of an individual: see section 10.

attribute service provider means an entity that provides, or proposes to provide, a service that verifies or 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) the Commonwealth, a State or a Territory;
(c) a body corporate incorporated by or under a law of the Commonwealth or a State or Territory;
(d) a Commonwealth entity, or a Commonwealth company, within the meaning of the *Public Governance, Performance and Accountability Act 2013*;
(e) a person or body that is an agency within the meaning of the *Freedom of Information Act 1982*;
(f) a body specified, or the person holding an office specified, in Part I of Schedule 2 to the *Freedom of Information Act 1982*;
(g) a department or authority of a State;
(h) a department or authority of a Territory;
(i) a partnership formed in Australia;
(j) a trust created in Australia;
(k) an unincorporated association that has its central management or control in Australia.

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.

credential service provider means an entity that provides, or proposes to provide, a service that does either or both of the following:

(a) generates, binds, manages or distributes credentials to an individual;

(b) binds, manages or distributes credentials generated by an individual.

cyber security incident has the meaning given by the TDI rules.

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

digital identity fraud incident has the meaning given by the TDI rules.

digital identity information means information that is:

(a) generated in a digital identity system; or

(b) obtained from a digital identity system; or

(c) collected for the purposes of a digital identity system.

digital identity system means a system that facilitates or manages either or both of the following in an online environment:

(a) the verification of the identity of individuals;

(b) the authentication of the digital identity of, or information about, individuals.

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 politic;
(c) a body corporate;
(d) a Commonwealth entity, or a Commonwealth company, within the meaning of the *Public Governance, Performance and Accountability Act 2013*;
(e) a person or body that is an agency within the meaning of the *Freedom of Information Act 1982*;
(f) a body specified, or the person holding an office specified, in Part I of Schedule 2 to the *Freedom of Information Act 1982*;
(g) a department or authority of a State;
(h) a department or authority of a Territory;
(i) a partnership;
(j) an unincorporated association;
(k) a trust.

identity exchange means a facility that conveys, manages and coordinates, or proposes to convey, manage and coordinate, the flow of data or other information between participants in a digital identity system.

identity service provider means an entity that provides, or proposes to provide, a service that generates, manages, maintains or verifies information relating to the identity of an individual.

interoperability obligation: see section 33.

onboarded: an entity is ***onboarded*** to the trusted digital identity system at a particular time if, at that time:
(a) the entity holds an approval under section 18 to onboard to the system; and
(b) either:
(i) the entity is directly connected to an accredited entity that is onboarded to the trusted digital identity system; or
(ii) the entity is an accredited entity that is directly connected to a participating relying party.

onboarding day for an entity means the day notified to the entity by the Oversight Authority for the purposes of paragraph 18(6)(c) as the day on which the entity must first onboard to the trusted digital identity system.

Oversight Authority means the Oversight Authority referred to in section 86.

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

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

(a) the relying party holds an approval under section 18 to onboard to the trusted digital identity system; and

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

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

(iii) whether the individual is alive or dead; and

(b) to the extent not already covered by paragraph (a), includes:

(i) an attribute of an individual; and

(ii) a restricted attribute of an individual; and

(iii) biometric information of an individual.

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

protected information: see subsection 103(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 identity service provider or attribute service provider 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 133.

Secretary means the Secretary of the Department.

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

(a) paragraph 18(2)(a);

(b) subsection 20(1);

(c) subsection 20(2);

(d) paragraph 22(2)(a);

(e) subsection 22(5);

(f) paragraph 24(2)(b);

(g) paragraph 28(2)(d);

(h) paragraph 29(1)(c);

(i) subsection 52(3);

(j) paragraph 53(2)(b);

(k) subsection 133(3).

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).

TDIF accreditation rules means rules made under section 157 for the purposes of the provisions in which the term occurs.

TDIF accredited entities register means the register kept under section 117.

TDIF trustmark: see subsection 84(2).

TDI rules means the rules made under section 157 for the purposes of the provisions in which the term occurs.

TDIS register means the register kept under section 118.

technical standards means the standards made under section 36.

this Act includes:

(a) the TDI rules; and

(b) the TDIF accreditation rules; and

(c) the Regulatory Powers Act as it applies in relation to this Act.

trusted digital identity advisory board: see section 106.

trusted digital identity system: see subsection 14(2).

trusted provider agreement: see section 35.

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 mobile phone number;

(f) the individual's email address;

(g) if the individual has a digital identity—the time and date the digital identity was created.

(3) However, the following is not an attribute of an individual:

(a) biometric information of the individual;

(b) a restricted attribute of the individual;

(c) 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) membership of a professional or trade association; or
(vii) membership of a trade union; or
(viii) sexual orientation or practices; or
(ix) criminal record;
(d) information that is prescribed by the TDI rules and relates to the individual.

(4) Subsection (3) does not prevent information described in any of the paragraphs in subsection (2) from being an attribute of an individual if the information is not primarily of any of the kinds described in subsection (3), even if information of any of those kinds can reasonably be inferred from the information.

Example: Even if an individual's racial or ethnic origin can reasonably be inferred from the individual's name or place of birth, this does not prevent the individual's name or place of birth from being an attribute of the individual.

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
(c) information that is prescribed by the TDI rules and relates to the individual.

(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 Oversight Authority must have regard to the matters (if any) specified in the TDI rules.

Chapter 2—The trusted digital identity system

Part 1—Introduction

13 Simplified outline of this Chapter

Part 2—The trusted digital identity system

Division 1—The trusted digital identity system

14 Oversight Authority may develop, operate and maintain the trusted digital identity system

(1) The Oversight Authority may develop, operate and maintain a digital identity system.

(2) The ***trusted digital identity system*** means the digital identity system developed, operated and maintained by the Oversight Authority under subsection (1).

15 Circumstances in which entities may onboard to the trusted digital identity system

(1) An entity mentioned in column 1 of an item in the following table may onboard to the trusted digital identity system if the entity satisfies the requirements set out in column 2 of that item.

Onboarding to the trusted digital identity system

Item	Column 1 Entity	Column 2 Requirements
1	Attribute service provider	(a) the attribute service provider: (i) must be an accredited attribute service provider; and (ii) must hold an approval under section 18 to onboard to the system; and (iii) if required by section 17—must have a trusted provider agreement with the Commonwealth; and

Onboarding to the trusted digital identity system		
Item	**Column 1** **Entity**	**Column 2** **Requirements**
		(b) the onboarding day for the attribute service provider must have arrived or passed
2	Credential service provider	(a) the credential service provider: (i) must be an accredited credential service provider; and (ii) must hold an approval under section 18 to onboard to the system; and (iii) if required by section 17—must have a trusted provider agreement with the Commonwealth; and (b) the onboarding day for the credential service provider must have arrived or passed
3	Identity exchange	(a) the identity exchange: (i) must be an accredited identity exchange; and (ii) must hold an approval under section 18 to onboard to the system; and (iii) if required by section 17—must have a trusted provider agreement with the Commonwealth; and (b) the onboarding day for the identity exchange must have arrived or passed
4	Identity service provider	(a) the identity service provider: (i) must be an accredited identity service provider;

Onboarding to the trusted digital identity system		
Item	**Column 1** **Entity**	**Column 2** **Requirements**
		and (ii) must have a trusted provider agreement with the Commonwealth; and (iii) must hold an approval under section 18 to onboard to the system; and (b) the onboarding day for the identity service provider must have arrived or passed
5	Relying party	(a) the relying party: (i) must be an Australian entity or a foreign registered company (within the meaning of the *Corporations Act 2001*); and (ii) must hold an approval under section 18 to onboard to the system; and (b) the onboarding day for the relying party provider must have arrived or passed
6	An entity of a kind prescribed by the TDIF accreditation rules for the purposes of paragraph 49(1)(e)	(a) the entity: (i) must be accredited as an accredited entity of that kind; and (ii) if required by section 17—must have a trusted provider agreement with the Commonwealth; and (iii) must hold an approval under section 18 to onboard to the system;

Onboarding to the trusted digital identity system		
Item	**Column 1** **Entity**	**Column 2** **Requirements**
		and (iv) must meet any other requirements prescribed by the TDI rules; and (b) the onboarding day for the entity must have arrived or passed

(2) An entity contravenes this subsection if:

(a) the entity connects to the trusted digital identity system; and

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

Civil penalty: 200 penalty units.

(3) An entity contravenes this subsection if:

(a) the entity connects to the trusted digital identity 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—Onboarding to the trusted digital identity system

16 Applying for approval to onboard to the trusted digital identity system

(1) The following kinds of entities may apply to the Oversight Authority for approval to onboard to the trusted digital identity system:

(a) an accredited entity;

(b) an entity that has applied for accreditation under section 49;

(c) subject to subsection (2)—a relying party.

Note 1: Only entities of particular kinds can be, or apply to be, an accredited entity (see subsection 49(2)).

Note 2: See Part 6 of Chapter 7 for matters relating to applications.

(2) If a relying party is not an Australian entity, the relying party cannot apply for onboarding to the trusted digital identity system unless the relying party is a registered foreign company (within the meaning of the *Corporations Act 2001*).

17 Applicants may be required to enter into trusted provider agreements

The Oversight Authority may, by written notice, require an applicant for onboarding to the trusted digital identity system (other than an identity service provider) to enter into a trusted provider agreement with the Commonwealth.

Note: All identity service providers must have a trusted provider agreement with the Commonwealth in order to onboard to the trusted digital identity system (see item 4 of the table in subsection 15(1)).

18 Approval to onboard to the trusted digital identity system

(1) The Oversight Authority may approve an entity to onboard to the trusted digital identity system if:

(a) the entity has made an application under section 16; and

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

(c) the Oversight Authority is satisfied that the entity will comply with the technical standards that apply in relation to the entity; and

(d) if section 17 applies to the entity or the entity is an identity service provider—the entity has entered into a trusted provider agreement with the Commonwealth; and

(e) if the Oversight Authority 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

(f) the Oversight Authority is satisfied that it is appropriate to approve the entity to onboard to the system; and

(g) any other requirements prescribed by the TDI rules are met.

(2) Without limiting paragraph (1)(f), the Oversight Authority 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.

Note: In having regard to whether an entity is a fit and proper person for the purposes of paragraph (c), the Oversight Authority may have regard to any matters specified in the TDI rules (see section 12).

(3) Without limiting paragraph (1)(g), the TDI rules may prescribe requirements relating to the security, reliability and stability of the trusted digital identity system.

(4) However, the Oversight Authority must not approve an entity to onboard to the trusted digital identity system if a direction under subsection 20(1) is in force in relation to the entity.

(5) The Oversight Authority must:

(a) give written notice of a decision to approve, or to refuse to approve, an entity to onboard to the trusted digital identity system; and

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

(6) If the Oversight Authority approves an entity to onboard to the trusted digital identity system, the notice must set out:

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

(b) any conditions imposed on the approval under subsection 22(4); and

(c) the day on which the entity must first onboard to the trusted digital identity system.

Note: It is a condition of the entity's approval that the entity onboard on the day referred to in paragraph (c) (see paragraph 22(1)(c)). An entity must not onboard before that day (see the requirements in column 2 of the table in subsection 15(1)).

19 Entities may be taken to be approved to onboard to the trusted digital identity system

The TDI rules may provide that a relying party is taken, for the purposes of this Act, to hold an approval under section 18 to onboard to the trusted digital identity system in the circumstances specified in the TDI rules.

20 Minister's directions regarding onboarding

(1) The Minister may, in writing, direct the Oversight Authority to refuse to approve the entity to onboard to the digital identity system under section 18 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 Oversight Authority to suspend the approval of an entity to onboard to the digital identity system under subsection 28(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 Oversight Authority must comply with the direction.

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

Note: The entity cannot be onboarded again while the direction remains in force (see subsection 18(4)).

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

21 Approval to onboard to the trusted digital identity system is subject to conditions

(1) The approval of an entity to onboard to the trusted digital identity system is subject to the following conditions (the ***approval conditions***):

(a) the conditions set out in subsection 22(1);

(b) the conditions (if any) imposed by the Oversight Authority under subsection 22(4), including as varied under subsection 24(1);

(c) the conditions (if any) determined by the TDI rules for the purposes of subsection 22(7).

Note: Failure to comply with a condition of approval may result in a suspension or revocation of the entity's approval (see sections 28 and 29).

(2) An entity that holds an approval to onboard to the trusted digital identity 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 onboard (see sections 28 and 29).

22 Conditions on approval to onboard to the trusted digital identity system

(1) The approval of an entity to onboard to the trusted digital identity 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—the entity must onboard to the trusted digital identity system only as the kind of entity in relation to which the entity is accredited;

(c) the entity must onboard to the trusted digital identity system on the entity's onboarding day;

(d) the entity must comply with this Act;

(e) the entity must comply with the technical standards that apply in relation to the entity;

(f) if entity has entered into a trusted provider agreement with the Commonwealth—the entity must comply with the agreement;

(g) the entity must comply with the service levels determined by the Oversight Authority under paragraph 87(c) or (d) that apply to the entity;

(h) the Oversight Authority is satisfied that it is appropriate for the entity to onboard to the trusted digital identity system.

(2) Without limiting paragraph (1)(h), the Oversight Authority may have regard to the following matters when considering whether it is appropriate for the entity to onboard to the trusted digital identity system:

(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.

Note: In having regard to whether an entity is a fit and proper person for the purposes of paragraph (b), the Oversight Authority may have regard to any matters specified in the TDI rules (see section 12).

(3) Without limiting paragraph (1)(i), the TDI rules may prescribe requirements relating to the security, reliability and stability of the trusted digital identity system.

(4) The Oversight Authority may impose conditions to which the approval of an entity to onboard to the trusted digital identity system is subject, either at the time of approval or at a later time, if the Oversight Authority considers that doing so is appropriate in the circumstances.

(5) Without limiting subsection (4), 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.

(6) Without limiting subsection (4), the conditions that the Oversight Authority may impose may relate to any of the following:

(a) the kind of accredited entity that the entity must directly connect to in order to onboard to the trusted digital identity system;

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

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

(d) the circumstances in which the entity may or must not provide services within the trusted digital identity system;

(e) for a relying party—the services the relying party is approved to provide, or to provide access to, within the trusted digital identity system;

(f) requirements to appoint personnel to undertake specified functions;

(g) actions that the entity must take before the entity's approval to onboard to the trusted digital identity system is suspended or revoked.

Note 1: For the purposes of paragraph (c), the Oversight Authority must have regard to the matters in subsection 23(2) before authorising an entity to obtain or disclose restricted attributes of individuals in the trusted digital identity system. If the Oversight Authority gives such an authorisation, the Oversight Authority must give a statement of reasons (see subsection 23(3)).

Note 2: An entity breaches this Act if the entity obtains or discloses restricted attributes of individuals in the trusted digital identity system and the entity's conditions of approval to onboard to the system do not authorise this (see section 74).

(7) The TDI rules may determine that each approval, or each approval included in a specified class of approval, to onboard to the trusted digital identity system is taken to include one or more specified conditions.

(8) Without limiting subsection (7), the TDI rules may provide that specified kinds of accredited entities are authorised to obtain or disclose specified kinds of restricted attributes of individual, either generally or in specified circumstances.

Note: The Minister must have regard to the matters in subsection 23(5) before making TDI rules for the purposes of this subsection.

23 Conditions relating to restricted attributes of individuals

Matters to which the Oversight Authority must have regard before authorising disclosure etc. of restricted attributes

(1) Subsection (2) applies if the Oversight Authority proposes to impose a condition on an entity's approval to onboard to the trusted digital identity system for the purposes of paragraph 22(6)(c) authorising the entity to obtain or disclose a restricted attribute of an individual in the trusted digital identity system.

(2) In deciding whether to impose the condition, the Oversight Authority 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 that was not authorised to obtain them;

(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 of the following information provided by the entity seeking authorisation to obtain 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 the relying party for the protection of the restricted attribute from further disclosure;

(e) any other matter the Oversight Authority considers relevant.

Requirement to give statement of reasons if authorisation given

(3) If the Oversight Authority imposes the condition, the Oversight Authority must publish a statement of reasons for giving the authorisation on the Oversight Authority's website.

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

(4) Subsection (5) applies if the Minister proposes to make TDI rules for the purposes of subsection 22(8) providing that specified kinds of accredited entities are authorised to obtain or disclose specified kinds of restricted attributes of individuals, either generally or in specified circumstances.

(5) In deciding whether to make the TDI 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 that was not authorised to obtain them;

(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 has been conducted in relation to the proposal to make the rules;

(e) any other matter the Minister considers relevant.

24 Variation and revocation of conditions

(1) The Oversight Authority may vary or revoke a condition imposed on an entity's approval under subsection 22(4):

(a) at any time, on the Oversight Authority's own initiative; or

(b) on application by the entity under section 27;

if the Oversight Authority considers it is appropriate to do so.

(2) Without limiting subsection (1), the Oversight Authority 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 trusted digital identity system;

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

25 Notice before changes to conditions on approval

(1) The Oversight Authority must not:

(a) impose a condition under subsection 22(4) on an entity's approval to onboard to the trusted digital identity system after the approval has been given; or

(b) vary or revoke a condition under subsection 24(1) on the Oversight Authority's own initiative;

unless the Oversight Authority 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 Oversight Authority, within the period specified in the notice, a written statement relating to the proposed condition, variation or revocation.

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

(a) impose a condition under subsection 22(4) on an entity's approval to onboard to the trusted digital identity system; or

(b) vary or revoke a condition under subsection 24(1) on an entity's approval to onboard to the trusted digital identity system.

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

26 Notice of decision of changes of conditions on approval

(1) Subject to subsection (2), the Oversight Authority must give an entity written notice of a decision to impose, vary or revoke a condition on an entity's approval to onboard to the trusted digital identity system.

(2) The Oversight Authority is not required to give an entity notice of the decision if notice of the condition was given in a notice under subsection 18(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.

27 Applying for variation or revocation of conditions on approval

(1) An entity that holds an approval to onboard to the trusted digital identity system may apply for a condition on the approval to be varied or revoked.

Note: See Part 6 of Chapter 7 for matters relating to applications.

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

Division 3—Suspension and revocation of approval to onboard

28 Suspension of approval to onboard to the trusted digital identity system

Oversight Authority must suspend approval if Minister's direction is in force

(1) The Oversight Authority must, in writing, suspend an approval given to an entity under section 18 if a direction under subsection 20(2) is in force in relation to the entity.

Oversight Authority may suspend approval in other circumstances

(2) The Oversight Authority may, in writing, suspend an approval given to an entity under section 18 if:

(a) the Oversight Authority reasonably believes that the entity has contravened or is contravening this Act; or

(b) the Oversight Authority reasonably believes that there has been a cyber security incident involving the entity; or

(c) the Oversight Authority reasonably believes that a cyber security incident involving the entity is imminent; or

(d) the Oversight Authority 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) circumstances specified in the TDI rules apply in relation to the entity.

(3) The Oversight Authority may, on application by an entity, suspend an approval given to the entity under section 18.

Note: See Part 6 of Chapter 7 for matters relating to applications.

Show cause notice must generally be given before decision to suspend

(4) Before suspending the approval of an entity under subsection (2), the Oversight Authority must give a written notice (a ***show cause notice***) to the entity.

(5) The show cause notice must:

(a) state the grounds on which the Oversight Authority proposes to suspend the entity's approval; and

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

Exception—cyber security incident or security

(6) Subsection (4) does not apply if the suspension is on a ground mentioned in paragraph (2)(b), (c) or (d).

Notice of suspension

(7) If the Oversight Authority suspends an entity's approval under subsection (1), (2) or (3), the Oversight Authority must give the entity a written notice stating the following:

(a) that the entity's approval to onboard to the trusted digital identity 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 onboard is suspended remains subject to certain obligations under this Act, including in relation to record keeping (see section 131) and the destruction or de-identification of personal information (see section 132). Such entities may also be subject to directions from the Oversight Authority (see sections 123 and 124).

Revocation of suspension

(8) 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.

(9) The Oversight Authority may revoke a suspension of an approval of an entity under subsection (2) by written notice to the entity.

(10) The Oversight Authority may revoke a suspension of an approval of an entity under subsection (3) by written notice to the entity, if the entity requests the suspension be revoked.

Effect of suspension

(11) If the approval of an entity to onboard to the trusted digital identity system is suspended under subsection (1), (2) or (3), the entity is taken not to hold the approval while it is suspended.

29 Revocation of approval to onboard to the trusted digital identity system

Oversight Authority may revoke approval

(1) The Oversight Authority may, in writing, revoke an approval given to an entity under section 18 if:

(a) the Oversight Authority reasonably believes that the entity has contravened or is contravening this Act; or

(b) the Oversight Authority reasonably believes that there has been a cyber security incident involving the entity; or

(c) the Oversight Authority 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) circumstances specified in the TDI rules apply in relation to the entity.

(2) The Oversight Authority must, on application by an entity, revoke an approval given to the entity under section 18. The revocation takes effect on the day determined by the Oversight Authority.

Note: See Part 6 of Chapter 7 for matters relating to applications.

Show cause notice must generally be given before decision to revoke

(3) Before revoking the approval of an entity under subsection (1), the Oversight Authority must give a written notice (a ***show cause notice***) to the entity.

(4) The show cause notice must:

(a) state the grounds on which the Oversight Authority proposes to revoke the entity's approval; and

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

Exception—cyber security incident or security

(5) Subsection (3) does not apply if the revocation is on a ground mentioned in paragraph (1)(b) or (c).

Notice of revocation

(6) If the Oversight Authority revokes an entity's approval under subsection (1) or (2), the Oversight Authority must give the entity a written notice stating the following:

(a) that the entity's approval to onboard the trusted digital identity 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 onboard has been revoked remains subject to certain obligations under this Act, including in relation to record keeping (see section 131) and the destruction or de-identification of personal information (see section 132). Such entities may also be subject to directions from the Oversight Authority (see section 123).

Approval can be revoked even while suspended

(7) Despite subsection 28(11), the Oversight Authority may revoke an entity's approval to onboard to the trusted digital identity system under this section even if a suspension is in force under section 28 in relation to the entity.

Division 4—Other matters relating to the trusted digital identity system

30 Generating and using a digital identity 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 generate or use a digital identity.

(2) 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 identity; or

(b) the participating relying party holds an exemption under subsection (3); or

(c) the participating relying party is of a kind covered by the TDI rules.

(3) Subject to subsection (5), the Oversight Authority may, on application by a participating relying party, grant an exemption under this subsection to the participating relying party if the Oversight Authority is satisfied that it is appropriate to do so.

Note: See Part 6 of Chapter 7 for matters relating to applications.

(4) Without limiting subsection (3), the Oversight Authority 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.

(5) However, the Oversight Authority must refuse to grant an exemption under subsection (3) to a participating relying party if the Oversight Authority is satisfied that:

(a) the participating relying party provides an essential service; or

(b) the participating relying party is the sole provider of services, or access to services, of that kind; or

(c) it is otherwise in the public interest to refuse to grant the exemption.

(6) For the purposes of paragraph (5)(a), ***essential services*** include emergency services, carriage services (within the meaning of the *Telecommunications Act 1997*), welfare services and the supply of electricity, gas and water.

(7) An exemption under subsection (3):

(a) must be in writing; and

(b) may be revoked by the Oversight Authority.

(8) The Oversight Authority 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.

31 Holding etc. digital identity information outside Australia

(1) The TDI rules may make provision in relation to the holding, storing, handling or transfer of digital identity information outside Australia if the information is or was generated, collected, held or stored by accredited entities within the trusted digital identity system.

(2) Without limiting subsection (1), the TDI 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 Oversight Authority to grant exemptions to entities from any such prohibitions; and

(c) may be expressed to apply to:

(i) entities that hold an approval to onboard to the trusted digital identity system; or

(ii) entities whose approval to onboard to the trusted digital identity system is suspended; or

(iii) entities whose approval to onboard to the trusted digital identity system has been revoked.

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

(a) the entity is subject to a requirement under the TDI rules made for the purposes of subsection (1); and

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

Civil penalty: 300 penalty units.

32 Reportable incidents

(1) The TDI 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 trusted digital identity system.

Note: The TDIF accreditation rules may also provide for such arrangements in relation to incidents that occur outside the trusted digital identity system (see subparagraph 59(2)(a)(ii)).

(2) Without limiting subsection (1), the TDI 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 Oversight Authority;

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

(f) how the Oversight Authority deals with reportable incidents, including action that may be taken by the Oversight Authority 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 Oversight Authority to the Minister, the Information Commissioner, accredited entities, participating relying parties or other specified bodies.

(3) Without limiting paragraph (2)(b), the TDI rules may specify the following kinds of incidents:

(a) digital identity 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 a service, or part of a service, for which the entity is accredited—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 TDI rules made for the purposes of subsection (1); and

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

Civil penalty: 300 penalty units.

33 Interoperability obligation

Meaning of interoperability obligation

(1) The matters set out in this section constitute the ***interoperability obligation***.

Participating relying parties must provide choice of accredited identity service providers

(2) Subsection (3) applies if:

(a) a participating relying party is seeking one or both of the following services:

(i) the verification of the identity of an individual;

(ii) the authentication of the digital identity of, or information about, an individual; and

(b) more than one accredited identity service provider:

(i) is onboarded to the trusted digital identity system; and

(ii) is accredited to provide the service at the level sought by the participating relying party.

Note: Conditions may be imposed on the accreditation of an accredited entity that limit the levels of identity proofing or levels or types of credentials that the entity can provide (see subsection 52(4)).

(3) The participating relying party must permit the individual to choose which of the accredited identity service providers provides the service to the participating relying party.

(4) Subsection (3) does not apply to a participating relying party if:

(a) the participating relying party has been granted an exemption under section 34; and

(b) if the exemption is subject to conditions—the participating relying party complies with the conditions.

Accredited entities must offer accredited services to every participating relying party and accredited entity

(5) An accredited entity that is onboarded to the trusted digital identity system must not refuse to provide the services for which it is accredited to another accredited entity or a participating relying party.

(6) Subsection (5) does not apply to an accredited credential service provider that is accredited to provide services only to accredited identity service providers.

(7) Subsection (5) does not apply to an accredited entity if:

(a) the accredited entity has been granted an exemption under section 34; and

(b) if the exemption is subject to conditions—the accredited entity complies with the conditions.

34 Exemption from interoperability obligation

(1) Subject to subsection (2), the Oversight Authority may, on application by a participating relying party or an accredited entity, grant an exemption from the interoperability obligation if the Oversight Authority considers it appropriate to do so.

Note: See Part 6 of Chapter 7 for matters relating to applications.

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

(3) The exemption:

(a) must be in writing; and

(b) must be for a specified period, which must not exceed 3 years; and

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

(4) An entity to whom a condition specified in an exemption applies must comply with the condition.

(5) The Oversight Authority may revoke an exemption granted under subsection (1) if the Oversight Authority considers it appropriate to do so.

35 Trusted provider agreements

(1) The Commonwealth may enter into a written agreement (a ***trusted provider agreement***) with an entity under which the entity is required to comply with obligations specified in the agreement in relation to the trusted digital identity system.

(2) Without limiting subsection (1), a trusted provider agreement may deal with the following:

(a) the terms on which the entity may charge fees in relation to the services it provides within the trusted digital identity system;

(b) administrative arrangements relating to the charging and payment of fees;

(c) the period for which the entity must provide, or offer to provide, services within the trusted digital identity system;
(d) how the agreement may be varied;
(e) how the agreement may be terminated.

(3) A trusted provider agreement must not be inconsistent with this Act.

36 Technical standards

(1) The Oversight Authority may, in writing, make standards (***technical standards***) relating to:
(a) technical integration requirements for entities to onboard to the trusted digital identity system; and
(b) technical or design features that entities must have to onboard to the trusted digital identity system.

(2) Without limiting subsection (1), the technical standards may deal with the following matters:
(a) the format and description of digital identity information that is generated, collected, used or disclosed by entities onboarded to the trusted digital identity system;
(b) technology requirements for disclosing digital identity information between entities within the trusted digital identity system.

(3) Without limiting subsection 33(3A) of the *Acts Interpretation Act 1901*, the technical standards may provide differently for different kinds of entities, things or circumstances.

(4) The Oversight Authority must publish the technical standards on the Oversight Authority's website.

(5) Technical standards made under subsection (1) are not a legislative instrument.

37 Entities may conduct testing in relation to the trusted digital identity system

(1) The Oversight Authority may authorise an entity, on application by the entity, to conduct testing in relation to the trusted digital identity system for the purposes of determining the entity's capability or suitability to onboard to the system.

Note: See Part 6 of Chapter 7 for matters relating to applications.

(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 Oversight Authority 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.

38 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 trusted digital identity system; and

(b) the accredited entity or another entity is authorised under section 37 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 onboarded entities

39 Accredited entities onboarded to the system protected from liability in certain circumstances

(1) If, while onboarded to the trusted digital identity system, an accredited entity:

(a) provides, or fails to provide, a service for which it is accredited; and

(b) provides, or fails to provide, the service to another accredited entity onboarded to the trusted digital identity system, or to a participating relying party; and

(c) provides, or fails to provide, the service in good faith, in compliance with this Act and with the technical standards that apply to the entity;

the entity is not liable to any action or other proceeding, whether civil or criminal, brought by an accredited entity or a participating relying party in relation to that service.

(2) An entity that wishes to rely on subsection (1) 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 contact

40 Statutory contract between entities onboarded to the system

(1) A contract is taken to be in force between:

(a) an accredited entity and every other accredited entity; and

(b) an accredited entity and each participating relying party;

under which each accredited entity agrees to provide the services for which it is accredited while onboarded to the trusted digital identity system, in compliance with the entity's obligations under this Act and with the technical standards, so far as those obligations and standards relate to the verification and authentication of individuals.

Note: This means an accredited entity will be taken to have a separate contract with every other accredited entity, and with each participating relying party.

(2) The contract is taken to be in force during the period:

(a) starting on the day that the onboarding day for both entities has arrived or passed; and

(b) ending on the day on which the approval to onboard to the trusted digital identity system has been revoked for at least one 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:

(i) the respondent; or

(ii) if the respondent is a body corporate—the directors of the body corporate;

about compliance with, or enforcement of, the contract;

(b) subject to any rules made for the purposes of subsection (5), 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 TDI rules may prescribe limits on the amount of compensation that an accredited entity is liable to pay under paragraph (4)(b).

41 Onboarded entities to maintain insurance as directed by Oversight Authority

(1) The Oversight Authority may, in writing, direct an accredited entity onboarded to the trusted digital identity system to maintain adequate insurance against any liabilities arising in connection with the obligations under section 40.

(2) If the Oversight Authority gives a direction to an entity under subsection (1), the direction is taken to be a condition imposed under subsection 22(4) on the entity's approval to onboard to the trusted digital identity system.

(3) A direction given under this section is not a legislative instrument.

42 Dispute resolution procedures

The TDI 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 40(3).

Division 3—Redress framework

43 Redress obligations of accredited entities

Accredited entities must contact individuals and businesses affected by an incident

(1) Subsection (2) applies if an accredited entity becomes aware that any of the following incidents has occurred or is occurring in relation to a service provided by the entity within the trusted digital identity system:

(a) a digital identity fraud incident;

(b) a cyber security incident.

(2) As soon as practicable after becoming aware of the incident, the accredited entity must make all reasonable efforts to contact:

(a) any individuals affected by the incident; and

(b) if the digital identity of an individual acting on behalf of a business has been compromised—that business.

Civil penalty: 200 penalty units.

(3) If the accredited entity is unable to contact the individual or business referred to in subsection (2), the entity must inform the Oversight Authority of that fact within 7 days of becoming aware of the incident.

Civil penalty: 200 penalty units.

Point of contact for affected individuals and businesses

(4) An accredited entity must:

(a) set up a point of contact to enable individuals to seek information and support about the occurrence, or suspected occurrence, of a digital identity fraud incident or a cyber security incident that has affected or may affect the individuals; and

(b) ensure that information regarding the point of contact is publicly available.

Policies dealing with incidents

(5) An accredited entity must have and maintain written policies dealing with the following:

(a) mechanisms and procedures for the management and resolution of digital identity fraud incidents and cyber security incidents;

(b) timeframes for managing and resolving such incidents.

Affected individuals and businesses to be kept informed

(6) If an individual or business is contacted by an accredited entity about an incident under subsection (2), the accredited entity must make all reasonable efforts to keep the individual or business informed in relation to the incident, including its management and resolution.

Civil penalty: 200 penalty units.

44 Redress obligations of participating relying parties

Participating relying parties must contact individuals and businesses affected by an incident

(1) Subsection (2) applies if a participating relying party becomes aware that any of the following incidents has occurred or is occurring in relation to a service the participating relying party is approved to provide in the trusted digital identity system:

(a) a digital identity fraud incident;

(b) a cyber security incident.

(2) As soon as practicable after becoming aware of the incident, the participating relying party must make all reasonable efforts to contact:

(a) any individuals affected by the incident; and

(b) if the digital identity of an individual acting on behalf of a business has been compromised—that business.

(3) If the participating relying party is unable to contact an individual or business referred to in subsection (2), the entity must inform the Oversight Authority of that fact within 7 days of becoming aware of the incident.

45 TDI rules may prescribe redress obligations

The TDI rules may prescribe additional obligations that accredited entities or participating relying parties must comply with in relation to the following matters:

(a) the identification of:

(i) digital identity fraud incidents; and

(ii) cyber security incidents; and

(iii) records or digital identities that have been compromised;

(b) procedures for dealing with any of the events described in subparagraphs (a)(i) to (iii), including the regeneration of a digital identity that has been compromised;

(c) the provision of assistance to individuals or businesses affected by digital fraud incidents or cyber security incidents.

Note: The TDIF accreditation rules may provide for similar obligations in relation to entities providing services outside of the trusted digital identity system.

46 Oversight Authority to assist individuals and businesses affected by incidents

If an individual is affected by a digital identity fraud incident or a cyber security incident, the Oversight Authority must provide reasonable assistance to such individuals and businesses, including by:

(a) informing individuals and businesses affected by the incident about support services available to them; and

(b) providing individuals and businesses affected by the incident with the contact details of the accredited entities and participating relying parties involved in the incident; and

(c) coordinating the collection of information from the trusted digital identity system that relates to a particular incident; and

(d) facilitating the sharing of information that relates to particular incidents between entities involved in the incident; and

(e) monitoring, and reporting on the nature and quality of the services provided by accredited entities and participating relying parties to individuals and businesses affected by an incident.

Section 47

Chapter 3—Accreditation

Part 1—Introduction

47 Simplified outline of this Chapter

Part 2—Accreditation

Division 1—Applying for accreditation

48 Authorisation to apply for accreditation

(1) The Oversight Authority may, on application by an entity, grant an authorisation to the entity to apply for accreditation as a specified kind of accredited entity if:

(a) the entity is of a kind mentioned in any of the paragraphs in paragraph 49(2)(b); and

(b) the Oversight Authority is satisfied that:

(i) the facility through which the entity proposes to provide the services for which it will seek accreditation is sufficiently developed; and

(ii) the entity has sufficient technical and financial resources available to it to become an accredited entity; and

(iii) the entity has an adequate plan for progressing to accreditation as an accredited entity.

Note 1: An entity must hold an authorisation under this section to be able to apply for accreditation as an accredited entity (see paragraph 49(2)(a)).

Note 2: See Part 6 of Chapter 7 for matters relating to applications.

(2) An authorisation under this section:

(a) must be in writing; and

(b) remains in force for 12 months, unless extended by the Oversight Authority for a further specified period (which must not exceed 12 months).

49 Applications for accreditation

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

(a) an accredited attribute service provider;
(b) an accredited credential service provider;
(c) an accredited identity exchange;
(d) an accredited identity service provider;
(e) an entity of a kind prescribed by the TDIF accreditation rules.

Note: See Part 6 of Chapter 7 for matters relating to applications.

(2) An entity is covered by this section if:
(a) the entity has been granted an authorisation under section 48 to apply for accreditation; and
(b) the entity is one of the following:
(i) the Commonwealth, a State or a Territory;
(ii) a body corporate incorporated by or under a law of the Commonwealth or a State or Territory;
(iii) a registered foreign company (within the meaning of the *Corporations Act 2001*);
(iv) a Commonwealth entity, or a Commonwealth company, within the meaning of the *Public Governance, Performance and Accountability Act 2013*;
(v) a person or body that is an agency within the meaning of the *Freedom of Information Act 1982*;
(vi) a body specified, or the person holding an office specified, in Part I of Schedule 2 to the *Freedom of Information Act 1982*;
(vii) a department or authority of a State;
(viii) a department or authority of a Territory.

Division 2—Accreditation

50 Oversight Authority must decide whether to accredit an entity

(1) This section applies if an entity has made an application under section 49 for accreditation as an accredited entity.

(2) The Oversight Authority must decide:
  (a) to accredit the entity; or
  (b) to refuse to accredit the entity.

(3) The Oversight Authority 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 credential service provider unless the entity is a credential service provider; or
  (c) as an accredited identity exchange unless the entity is an identity exchange; or
  (d) as an accredited identity service provider unless the entity is an identity service provider; or
  (e) if rules made for the purposes of paragraph 49(1)(e) prescribe an entity—as an entity of that kind unless the entity is an entity of that kind.

(4) Before deciding whether to accredit or refuse to accredit the entity, the Oversight Authority may consult the Information Commissioner.

(5) In deciding whether to accredit the entity, the Oversight Authority:
  (a) must be satisfied that the entity will comply with this Act; and
  (b) if the Oversight Authority makes a requirement under paragraph 126(1)(a) in relation to the entity—must be satisfied that the entity has been assessed as being able to comply with this Act; and
  (c) must have regard to the matters (if any) prescribed by the TDIF accreditation rules; and

(d) may have regard to the following:
(i) matters raised in consultations (if any) under subsection (4);
(ii) whether the entity is a fit and proper person;
(iii) any other matters the Oversight Authority considers relevant.

Note: In having regard to whether an entity is a fit and proper person for the purposes of subparagraph (d)(ii), the Oversight Authority may have regard to any matters specified in the TDI rules (see section 12).

(7) The Oversight Authority 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.

(8) If the Oversight Authority 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 of accreditation imposed under subsection 52(2).

51 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 52(1);
(b) the conditions (if any) imposed by the Oversight Authority under subsection 52(2), including as varied under subsection 53(1);
(c) the conditions (if any) determined by the TDIF accreditation rules under subsection 52(5).

Note: Failure to comply with a condition of accreditation may result in a suspension or revocation of the entity's accreditation (see sections 57 and 58).

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

Note: Failure to comply with a condition of accreditation may result in a suspension or revocation of the entity's accreditation (see sections 57 and 58).

52 Conditions of accreditation

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

(2) The Oversight Authority may impose conditions to which the accreditation of an entity is subject, either at the time of accreditation or at a later time, if the Oversight Authority considers that doing so is appropriate in the circumstances.

(3) 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.

(4) Without limiting subsection (2), the conditions that the Oversight Authority may impose may relate to the following:

(a) the biometric information (if any) the entity is authorised to collect, use or disclose;

(b) the levels of identity proofing that the entity is authorised to provide;

(c) the levels or types of credentials the entity is authorised to provide;

(d) the entity's accredited facility, including restrictions on changes to the facility;

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

(5) The TDIF accreditation rules may determine that each accreditation, or each accreditation included in a specified class of accreditation, is taken to include one or more specified conditions.

53 Variation and revocation of conditions of accreditation

(1) The Oversight Authority may vary or revoke a condition imposed on an entity's accreditation under subsection 52(2):

(a) at any time, on the Oversight Authority's own initiative; or

(b) on application by the entity under section 56;

if the Oversight Authority considers it is appropriate to do so.

(2) Without limiting subsection (1), the Oversight Authority 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 trusted digital identity system;

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

54 Notice before changes to conditions on accreditation

(1) The Oversight Authority must not:

(a) impose a condition under subsection 52(2) on an entity's accreditation after the entity has been accredited; or

(b) vary or revoke a condition under subsection 53(1) on the Oversight Authority's own initiative;

unless the Oversight Authority 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 Oversight Authority, within the period specified in the notice, a written statement relating to the proposed condition, variation or revocation.

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

(a) impose a condition under subsection 52(2) on an entity's accreditation; or

(b) vary or revoke a condition under subsection 53(1) on an entity's accreditation.

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

55 Notice of decision of changes to conditions on accreditation

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

(2) The Oversight Authority is not required to give an entity notice of the decision if notice of the condition was given in a notice under subsection 50(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.

56 Applying for variation or revocation of conditions on accreditation

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

Note: See Part 6 of Chapter 7 for matters relating to applications.

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

Division 3—Suspension and revocation of accreditation

57 Suspension of accreditation

Oversight Authority may decide to suspend accreditation

(1) The Oversight Authority may, in writing, suspend the accreditation of an accredited entity if:

(a) the Oversight Authority reasonably believes that the accredited entity has contravened or is contravening this Act; or

(b) the Oversight Authority reasonably believes that there has been a cyber security incident involving the entity; or

(c) the Oversight Authority reasonably believes that a cyber security incident involving the entity is imminent; or

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

(e) circumstances specified in the TDIF accreditation rules apply in relation to the entity.

(2) The Oversight Authority must, on application by an accredited entity, suspend the accreditation of the entity.

Note: See Part 6 of Chapter 7 for matters relating to applications.

Show cause notice must generally be given before decision to suspend

(3) Before suspending the accreditation of an entity under subsection (1), the Oversight Authority must give a written notice (a ***show cause notice***) to the entity.

(4) The show cause notice must:

(a) state the grounds on which the Oversight Authority proposes to suspend the entity's accreditation; and

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

showing cause why the Oversight Authority should not suspend the accreditation.

Exception—cyber security incident

(5) Subsection (3) does not apply if the suspension is on a ground mentioned in paragraph (1)(b) or (c).

Notice of suspension

(6) If the Oversight Authority decides to suspend an entity's accreditation under subsection (1) or (2), the Oversight Authority 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.

Revocation of suspension

(7) The Oversight Authority may revoke a suspension of an entity's accreditation under subsection (1) by written notice to the entity. The notice must specify the day the revocation takes effect.

(8) The Oversight Authority must revoke a suspension of an entity's accreditation under subsection (2) by written notice to the entity, if the entity requests the suspension be revoked. The notice must specify the day the revocation takes effect.

Effect of suspension

(9) If an entity's accreditation is suspended under subsection (1) or (2), the entity is taken not to be accredited while the suspension is in force.

58 Revocation of accreditation

(1) The Oversight Authority may, in writing, revoke an entity's accreditation if:

(a) the Oversight Authority reasonably believes that the accredited entity has contravened or is contravening this Act; or

(b) the Oversight Authority reasonably believes that there has been a cyber security incident involving the entity; or

(c) the Oversight Authority reasonably believes that a cyber security incident involving the entity is imminent; or

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

(e) circumstances specified in the TDIF accreditation rules apply in relation to the entity.

(2) The Oversight Authority may, on application by an entity, revoke the entity's accreditation. The revocation takes effect on the day determined by the Oversight Authority.

Note: See Part 6 of Chapter 7 for matters relating to applications.

Show cause notice must generally be given before decision to revoke

(3) Before revoking the accreditation of an entity under subsection (1), the Oversight Authority must give a written notice (a ***show cause notice***) to the entity.

(4) The show cause notice must:

(a) state the grounds on which the Oversight Authority proposes to revoke the entity's accreditation; and

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

Exception—cyber security incident

(5) Subsection (3) does not apply if the revocation is on a ground mentioned in paragraph (1)(b) or (c).

Notice of revocation

(6) If the Oversight Authority decides to revoke an entity's accreditation under subsection (1) or (2), the Oversight Authority 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.

Approval can be revoked even while suspended

(7) Despite subsection 57(9), the Oversight Authority may revoke an entity's accreditation under this section even if a suspension is in force under section 57 in relation to the entity.

Division 4—TDIF accreditation rules

59 TDIF accreditation rules

(1) The TDIF 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 TDIF 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;

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

(c) the conduct of periodic reviews of an entity's compliance with specified requirements of the TDIF accreditation rules, including the timing of such reviews, who is to conduct such reviews and the provision of reports about such reviews to the Oversight Authority;

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

(e) requirements relating to the collection, use and disclosure of attributes of individuals;

(f) requirements relating to the collection, use and disclosure of restricted attributes of individuals;

(g) the kinds of biometric information that may be collected, used or disclosed by accredited entities and quality and security requirements that apply;

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

60 TDIF accreditation rules may incorporate etc. material as in force or existing from time to time

(1) Despite subsection 14(2) of the *Legislation Act 2003*, the TDIF accreditation rules 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.

(2) If the TDIF accreditation rules make provision in relation to a matter in accordance with subsection (1), the TDIF rules may also make provision in relation to when changes to an incorporated instrument take effect for the purposes of the rules.

Division 5—Other matters relating to accredited entities

61 Digital identities must be deactivated on request

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

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

62 Services provided by accredited entities must be accessible and inclusive

(1) The TDIF accreditation rules must provide for and in relation to requirements relating to the accessibility and useability of the services for which accredited entities are accredited to provide.

(2) Without limiting subsection (1), the TDIF 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 4—Privacy

Part 1—Introduction

63 Simplified outline of this Chapter

Part 2—Privacy

Division 1—Interaction with the Privacy Act 1988

64 Extended meaning of *personal information*

To the extent not already covered by the definition of ***personal information*** within the *Privacy Act 1988*, the following are taken, for the purposes of that Act, to be personal information about an individual:

(a) attributes of individuals;

(b) restricted attributes of individuals;

(c) biometric information of individuals.

Note 1: This section has the effect of extending the meaning of personal information in the *Privacy Act 1988* 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 information of the kind mentioned in paragraphs (a), (b) and (c).

65 Privacy obligations for non-APP entities

(1) This section applies to an entity if:

(a) the entity is an accredited entity; and

(b) the entity is not an APP entity.

Note 1: The obligations of entities that are APP entities in relation to the handling of personal information are set out in the *Privacy Act 1988*.

Note 2: See section 9 for the definition of ***personal information***. Section 64 extends the meaning of that term in the *Privacy Act 1988* to mirror its meaning in this Act.

(2) The entity must not do an act or engage in a practice with respect to personal information for the purposes of this Act 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 a trusted provider agreement with the Commonwealth;

(iii) the agreement prohibits the entity from collecting, 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.

66 Contraventions of Division 2 are interferences with privacy

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

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

(b) covered by section 13 of that Act.

Note 1: See section 9 for the definition of ***personal information***. Section 64 extends the meaning of that term in the *Privacy Act 1988* to mirror its meaning in this Act.

Note 2: An act or practice that is 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 an 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) If:

(a) an act or practice of an 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 (within the meaning of that Act) or organisation (within the meaning of that Act);

the entity is taken, for the purposes of that Part and any other provision of that Act that relates to that Part, to be an organisation (within the meaning of that Act).

67 Notification of eligible data breaches—accredited entities that are APP entities

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

(a) is an accredited entity; and

(b) is an APP entity; and

(c) 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 services the entity is accredited to provide; 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 Oversight Authority at the same time as the statement is given to the Information Commissioner.

68 Notification of eligible data breaches—accredited entities (other than State or Territory bodies) that are not APP entities

(1) This section applies to an entity if:

(a) the entity is an accredited entity; and

(b) the entity is not an APP entity.

(2) Despite paragraph (1)(b), this section does not apply to an 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 69 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 entity as if the entity were an APP entity.

(4) If:

(a) the 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 services the entity is accredited to provide; 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 copy (the ***first copy***) of a statement that complies with subsection 26WK(3) of that Act;

the entity must also give a copy of the statement to the following at the same time as the first copy is given to the Information Commissioner:

(a) the Oversight Authority;

(b) the State or Territory privacy authority that has jurisdiction in relation to the entity.

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

(1) This section applies to an entity if:

(a) the entity is an accredited entity; and
(b) the entity is not an APP entity; and
(c) the entity is a department or authority of a State or Territory; and
(d) 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
(e) the statement relates to the services the entity is accredited to provide.

(2) The entity must also give a copy of the statement to the Oversight Authority at the same time as the statement is given to the notified entity.

70 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 Oversight Authority, on matters relating to the operation of this Act.

71 Information Commissioner may disclose details of investigations to Oversight Authority

The Information Commissioner is authorised to disclose to the Oversight Authority any information or documents that relate to an investigation the Information Commissioner conducts because of the operation of section 66, if the Information Commissioner is satisfied that to do so will enable the Oversight Authority to:

(a) monitor or improve the operation or security of the trusted digital identity system; or
(b) ensure compliance with this Act by accredited entities.

72 Commissioner may share information with State or Territory privacy authorities

(1) Subject to subsection (2), the Information Commissioner may share information or documents with a State or Territory privacy authority:

(a) for the purpose of the Information Commissioner exercising powers, or performing functions or duties under this Act, or under the *Privacy Act 1988* in connection with this Act; or

(b) for the purpose of the State or Territory privacy authority exercising its powers, or performing its functions or duties.

(2) The Information Commissioner may only share information or documents with a State or Territory privacy authority under this section if:

(a) the information or documents were acquired by the Information Commissioner in the course of exercising powers, or performing functions or duties, under this Act or under the *Privacy Act 1988* in connection with this Act; and

(b) the Information Commissioner is satisfied that the State or Territory privacy authority has satisfactory arrangements in place for protecting the information or documents.

(3) To avoid doubt, the Information Commissioner may share information or documents with a State or Territory privacy authority under this section whether or not the Information Commissioner is transferring a complaint, or part of a complaint, made under Part V of the *Privacy Act 1988* to the authority.

Division 2—Additional privacy safeguards

73 Individuals must expressly consent to disclosure of attributes of individuals to relying parties

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

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

(a) the entity contravenes subsection (1); and

(b) the contravention occurs within the trusted digital identity system.

Civil penalty: 300 penalty units.

74 Disclosure of restricted attributes of individuals

(1) When verifying the identity of an individual or authenticating the digital identity 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.

(2) An accredited entity must not disclose a restricted attribute of an individual to a participating relying party if the participating relying party's conditions of onboarding to the trusted digital identity system do not include an authorisation to obtain the restricted attribute.

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

(a) the entity contravenes subsection (1) or (2); and

(b) the contravention occurs within the trusted digital identity system.

Civil penalty: 300 penalty units.

75 Prohibition on single identifiers

(1) This section applies if:

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

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

(2) The assigning accredited entity must not provide the unique identifier to any other entity.

(3) The receiving accredited entity must not provide the unique identifier to any other entity.

(4) Subsections (2) and (3) do not apply if the provision of the unique identifier:

(a) is for the purposes of detecting, reporting, investigating or conducting proceedings in relation to a contravention, or an alleged contravention, of a civil penalty provision of this Act; or

(b) is for the purposes of the Oversight Authority detecting, reporting or investigating a contravention, or an alleged contravention, of subsection (2) or (3); or

(c) is for the purposes of detecting, reporting, investigating or prosecuting an offence against a law of the Commonwealth.

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

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

(a) the entity contravenes subsection (2) or (3); and

(b) the contravention occurs within the trusted digital identity system.

Civil penalty: 300 penalty units.

76 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 77 or 78; and

(b) the individual to whom the information relates has expressly consented to the collection, use or disclosure.

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

(a) disclose biometric information of an individual to an enforcement body; or

(b) collect, use or disclose biometric information of an individual to identify the individual; or

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

(3) Paragraph (2)(a) applies despite any law of the Commonwealth, a State or a Territory (whether enacted or made before or after this section) or a warrant, authorisation or order issued under such a law.

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

(a) the entity contravenes subsection (1); and

(b) the contravention occurs within the trusted digital identity system.

Civil penalty: 300 penalty units.

77 Authorised collection, use and disclosure of biometric information of an individual—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 or an accredited credential service provider; and

(b) the entity's conditions of 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:

(i) verifying the identity of the individual; or

(ii) authenticating the individual to their digital identity.

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

(3) An accredited entity is authorised to retain and use biometric information of an individual if:

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

(b) the entity collected the information under subsection (1); and

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

(d) the entity complies with the requirements prescribed by the TDIF accreditation rules.

(4) Without limiting paragraph (3)(d), TDIF accreditation rules made for the purposes of that paragraph must 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 biometric information may be undertaken;

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

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

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

(g) reporting of testing results to the Oversight Authority.

(5) An accredited entity is authorised to retain and use biometric information of an individual if:

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

(b) the entity collected the information under subsection (1); and

(c) the information is retained and used for the purposes of preventing or detecting a digital identity fraud incident; and

(d) the entity complies with the requirements prescribed by the TDIF accreditation rules.

(6) Without limiting paragraph (5)(d), TDIF accreditation rules made for the purposes of that paragraph must prescribe requirements in relation to the following matters:

(a) the manner in which biometric information that has been retained for preventing or detecting digital identity fraud incidents must be deleted;

(b) the reporting of fraud prevention and detection activities to the Oversight Authority.

78 Government entities collecting etc. biometric information for other purposes

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

(a) is an accredited identity service provider or an accredited credential service provider; and

(b) is one of the following:

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

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

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

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

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

(vi) a department or authority of a State;

(vii) a department or authority of a Territory; and

(c) collects biometric information of an individual under subsection 77(1).

(2) The entity is authorised to collect, use or disclose the information for the purposes of issuing a document or other thing that:

(a) contains personal information about the individual; and

(b) can be used to assist the individual to prove the individual's age or identity; and

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

79 Deletion of biometric information of individuals

(1) If an accredited identity service provider obtains biometric information of an individual for the purposes of verifying an individual's identity, the provider must delete the information immediately after the verification is complete.

(2) If:

(a) an accredited credential service provider obtains biometric information of an individual with the express consent of the individual to whom the information relates; and

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

(c) the individual withdraws their consent;

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

(3) If an accredited entity retains biometric information of an individual under subsection 77(3) (about testing), the entity must delete the information at the earlier of:

(a) the completion of testing the information; and

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

(4) If an accredited entity retains biometric information of an individual under subsection 77(5) (about preventing or detecting digital identity fraud incidents), the entity must delete the information at the earlier of:

(a) the prevention or detection of the digital identity fraud incident; and

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

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

(a) the entity contravenes this section; and

(b) the contravention occurs within the trusted digital identity system.

Civil penalty: 300 penalty units.

80 Prohibition on data profiling

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

(a) the information is digital identity information held in the entity's accredited facility; and

(b) the information is any of the following:

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

(ii) information relating to how or when access was obtained or attempted;

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

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

(2) Subsection (1) does not apply if the use or disclosure:

(a) is for the purposes of providing the services for which the entity is accredited; or

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

(c) subject to subsection (3)—is required or authorised by or under a law of the Commonwealth, a State or a Territory.

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

(3) Despite paragraph (2)(c), the following do not authorise the use or disclosure of information for the purposes of that paragraph:

(a) paragraph 6.1(a) of Australian Privacy Principle 6 (about consent);

(b) an equivalent principle or law of a State or Territory.

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

(a) the entity contravenes subsection (1); and

(b) the contravention occurs within the trusted digital identity system.

Civil penalty: 300 penalty units.

81 Digital identity information must not be used for prohibited enforcement purposes

(1) An accredited entity must not use or disclose digital identity information held in the entity's accredited facility if:

(a) the information is used or disclosed for the purposes of enforcement related activities conducted by, or on behalf of, an enforcement body; and

(b) none of the following apply:

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

(ii) at the time the information is used or disclosed, 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;

(iii) the information is used or disclosed under a warrant issued under a law of the Commonwealth, a State or a Territory.

(2) Subsection (1) 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.

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

(a) the entity contravenes subsection (1); and

(b) the contravention occurs within the trusted digital identity system.

Civil penalty: 300 penalty units.

82 Digital identity information must not be used or disclosed for prohibited marketing purposes

(1) An accredited entity must not use or disclose digital identity information held in the entity's accredited facility if the information is used or disclosed for the purposes of:

(a) offering to supply goods or services; or

(b) advertising or promoting goods or services; or

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

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

(e) market research.

(2) Subsection (1) does not apply to the disclosure of information if:

(a) the information is disclosed for the purposes of offering to supply services or advertising or promoting services that the entity is accredited to provide; and

(b) the individual to whom the information is disclosed has expressly consented to the disclosure.

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

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

(a) the entity contravenes subsection (1); and

(b) the contravention occurs within the trusted digital identity system.

Civil penalty: 300 penalty units.

83 Accredited identity exchanges must not retain attributes or restricted attributes of individuals

(1) This section applies if an accredited identity exchange receives either of the following during an authenticated session:

(a) an attribute of an individual;

(b) a restricted attribute of an individual.

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

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

(a) the entity contravenes subsection (2); and

(b) the contravention occurs within the trusted digital identity system.

Civil penalty: 300 penalty units.

(4) In this section:

authenticated session has the meaning given by the TDIF accreditation rules.

Chapter 5—TDIF trustmarks

84 TDIF trustmarks

(1) The TDI rules may do one or more of the following:

(a) specify one or more TDIF trustmarks that may be used by accredited entities;

(b) specify one or more TDIF trustmarks that may be used by participating relying parties;

(c) prescribe conditions in relation to the use and display of those TDIF trustmarks.

(2) ***TDIF trustmark*** means a mark, symbol, logo or design set out in the TDI rules.

85 Authorised use of TDIF trustmarks etc.

(1) An entity is authorised to use a TDIF trustmark if:

(a) the TDI rules permit the entity to use the TDIF trustmark; and

(b) if the TDI rules prescribe conditions in relation to the use or display of the TDIF trustmark—the entity complies with the conditions.

(2) An entity must not use a TDIF 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 TDIF trustmark as to be likely to be mistaken for it:

(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.

Chapter 6—Oversight Authority

Part 1—Oversight Authority

Division 1—Establishment and functions of the Oversight Authority

86 Oversight Authority

There is to be an Oversight Authority.

87 Functions of the Oversight Authority

The Oversight Authority has the following functions:

(a) to identify and manage risks in relation to the trusted digital identity system;

(b) to manage the design of the trusted digital identity system and the process for coordinating outages, including to ensure that changes made by onboarded entities do not adversely affect the system as a whole;

(c) to determine service levels for accredited entities that hold an approval to onboard to the trusted digital identity system relating to the availability and performance of the entity's accredited facility;

(d) to determine service levels for participating relying parties relating to the availability and performance of each service the participating relying party is approved to provide, or provide access to;

(e) to establish and operate a test environment for the trusted digital identity system, and other electronic systems that interact directly with the trusted digital identity system, in accordance with the requirements (if any) specified in the TDI rules;

(f) to advise and assist entities in relation to their obligations under this Act;

(g) to promote compliance with this Act;

(h) to consult, cooperate with, and provide guidance to entities in relation to digital identity matters;

(i) to support, encourage, conduct and evaluate educational, promotional and community awareness programs that are relevant to digital identity matters;

(j) to advise the Minister, either on its own initiative or on request, on matters relating to any of the Oversight Authority's functions;

(k) to refer matters arising under this Act to the Australian Federal Police or the police force of a State or Territory;

(l) to facilitate, as required by law, access to information by law enforcement agencies (within the meaning of the *Australian Crime Commission Act 2002*) or any other agency or body of the Commonwealth, a State or a Territory;

(m) such other functions as are conferred on the Oversight Authority by or under this Act or any other law of the Commonwealth;

(n) to do anything that is incidental or conducive to the performance of any of the above functions.

88 Powers of the Oversight Authority

The Oversight Authority has power to do all things necessary or convenient to be done for or in connection with the performance of its functions.

89 Independence of Oversight Authority

Subject to this Act and other laws of the Commonwealth, the Oversight Authority has discretion in the performance or exercise of the Oversight Authority's functions or powers and is not subject to direction by any person in relation to the performance or exercise of those functions or powers.

Note: The Minister may direct the Oversight Authority to refuse to approve or suspend the onboarding of entities (see section 20).

Division 2—Appointment of the Oversight Authority

90 Appointment

(1) The Oversight Authority is to be appointed by the Minister by written instrument.

Note: The Oversight Authority may be reappointed: see section 33AA of the *Acts Interpretation Act 1901*.

(2) The Oversight Authority is to be appointed on a full-time basis.

91 Term of appointment

The Oversight Authority holds office for the period specified in the instrument of appointment. The period must not exceed 5 years.

92 Acting Oversight Authority

The Minister may, by written instrument, appoint a person to act as the Oversight Authority:

(a) during a vacancy in the office of the Oversight Authority (whether or not an appointment has previously been made to the office); or

(b) during any period, or during all periods, when the Oversight Authority:

(i) is absent from duty or from Australia; or

(ii) is, for any reason, unable to perform the duties of the office.

Note: Sections 33AB and 33A of the *Acts Interpretation Act 1901* have rules that apply to acting appointments.

93 Application of the finance law

The Oversight Authority is an official of the Department for the purposes of the finance law (within the meaning of the *Public Governance, Performance and Accountability Act 2013*).

Division 3—Terms and conditions for the Oversight Authority

94 Remuneration

(1) The Oversight Authority 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 Oversight Authority is to be paid the remuneration that is prescribed by legislative instrument under subsection (3).

(2) The Oversight Authority 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) This section has effect subject to the *Remuneration Tribunal Act 1973*.

95 Leave of absence

(1) The Oversight Authority has the recreation leave entitlements that are determined by the Remuneration Tribunal.

(2) The Minister may grant the Oversight Authority leave of absence, other than recreation leave, on the terms and conditions as to remuneration or otherwise that the Minister determines.

96 Outside work

The Oversight Authority must not engage in paid work outside the duties of the Oversight Authority's office without the Minister's approval.

97 Disclosure of interests

(1) The Oversight Authority must give written notice to the Minister of any direct or indirect pecuniary interest that the Oversight Authority has or acquires and that conflicts or could conflict with the proper performance of the Oversight Authority'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).

98 Resignation of appointment

(1) The Oversight Authority may resign the Oversight Authority'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.

99 Suspension or termination of appointment

(1) The Minister may suspend or terminate the appointment of the Oversight Authority:
  (a) for misbehaviour; or
  (b) if the Oversight Authority is unable to perform the duties of the Oversight Authority's office because of physical or mental incapacity.

(2) The Minister may suspend or terminate the appointment of Oversight Authority if:
  (a) the Oversight Authority:
    (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 Oversight Authority's creditors; or
    (iv) makes an assignment of the Oversight Authority's remuneration for the benefit of the Oversight Authority's creditors; or

(b) the Oversight Authority is absent, except on leave of absence, for 14 consecutive days or for 28 days in any 12 months; or

(c) the Oversight Authority engages, except with the Minister's approval, in paid work outside the duties of the Oversight Authority's office (see section 96); or

(d) the Oversight Authority 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.

Division 4—Staff assisting the Oversight Authority

100 Staff

(1) The staff assisting the Oversight Authority are to be APS employees in the Department whose services are made available to the Oversight Authority by the Secretary of the Department in connection with the performance of any of the Oversight Authority's functions.

(2) When performing services for the Oversight Authority, the persons are subject to the directions of the Oversight Authority.

101 Consultants

(1) The Oversight Authority may, on behalf of the Commonwealth, engage persons having suitable qualifications and experience as consultants to assist in the performance of the functions and the exercise of the powers of the Oversight Authority.

(2) The consultants are to be engaged on the terms and conditions that the Oversight Authority determines in writing.

102 Contractors

(1) The Oversight Authority may, on behalf of the Commonwealth, engage persons under a written agreement to assist the Oversight Authority in the performance of the functions and the exercise of the powers of the Oversight Authority.

(2) The persons are to be engaged on the terms and conditions that the Oversight Authority determines in writing.

Division 5—Protecting personal and commercially sensitive information

103 Prohibition on Oversight Authority and staff using or disclosing personal or commercially sensitive information

Offence

(1) A person commits an offence if:

(a) the person is or has been a person mentioned in subsection (2); 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 apply:

(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) The persons are as follows:

(a) the Oversight Authority;

(b) a person whose services are made available to the Oversight Authority under section 100;

(c) a person engaged by the Oversight Authority under section 101 or 102.

Exception—authorised use or disclosure

(3) Subsection (1) does not apply if the use or disclosure is authorised by section 104 (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.

104 Authorised uses and disclosures of personal or commercially sensitive information

(1) A 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 Australian law; or

(b) the use or disclosure is required or authorised by or under:

(i) a Commonwealth law (including this Act); or

(ii) a law, of a State or Territory, that is prescribed by the TDI rules; or

(c) the person referred to in subparagraph 103(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 TDI rules; or

(f) both:

(i) the 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.

105 Disclosing personal or commercially sensitive information to courts and tribunals etc.

(1) Except where it is necessary to do so for the purposes of giving effect to this Act, a 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 apply:

(c) the information is personal information of an individual other than the 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 boards and committees

106 Establishment and functions of trusted digital identity advisory board

(1) The Minister must establish, in writing, an advisory board (the ***trusted digital identity advisory board***) to advise the Oversight Authority in relation to the performance of the Oversight Authority's functions or the exercise of the Oversight Authority's powers under this Act.

(2) The trusted digital identity board must not advise the Oversight Authority in relation to:

(a) a decision on a particular application made under this Act; or

(b) the operation of the TDIF accreditation rules.

107 Trusted digital identity advisory board members

Appointment

(1) Each member of the trusted digital identity advisory board is to be appointed by the Minister by written instrument, on a part-time basis.

Note: A member may be reappointed: see section 33AA of the *Acts Interpretation Act 1901*.

(2) A person may only be appointed as a member of the trusted digital identity advisory board if the Minister is satisfied that the person has appropriate qualifications, knowledge or experience.

Term of appointment

(3) A member of the trusted digital identity advisory board holds office for the period specified in the instrument of appointment. The period must not exceed 3 years.

108 Trusted digital identity advisory board members—remuneration

(1) A member of the trusted digital identity advisory board 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 member is to be paid the remuneration that is prescribed by legislative instrument under subsection (3).

(2) A member of the trusted digital identity advisory board is to be paid the allowances as 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) This section has effect subject to the *Remuneration Tribunal Act 1973*.

109 Trusted digital identity advisory board members—leave of absence

The Minister may grant leave of absence to a member of the trusted digital identity advisory board on the terms and conditions that the Minister determines.

110 Outside employment

A member of the trusted digital identity advisory board must not engage in any paid work that, in the opinion of the Minister, conflicts or could conflict with the proper performance of the member's duties.

111 Trusted digital identity advisory board members—disclosure of interests

(1) A member of the trusted digital identity advisory board must give written notice to the Minister of all interests, pecuniary or

otherwise, that the member has or acquires and that conflict or could conflict with the proper performance of the member's office as a member of the board.

(2) A member of the trusted digital identity advisory board who has an interest, pecuniary or otherwise, in a matter being considered or about to be considered by the board must disclose the nature of the interest to a meeting of the board.

(3) The disclosure must be made as soon as possible after the relevant facts have come to the member's knowledge.

(4) The disclosure must be recorded in the minutes of the meeting.

112 Trusted digital identity advisory board members—resignation and termination

Resignation

(1) A member of the trusted digital identity advisory board may resign from the board 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.

Termination

(3) The Minister may terminate the appointment of a member of the trusted digital identity advisory board:

(a) for misbehaviour; or

(b) if the member is unable to perform the duties of a member of the board because of physical or mental incapacity; or

(c) if the member:

(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 member's creditors; or

(iv) makes an assignment of the member's remuneration for the benefit of the member's creditors; or

(d) if the member is absent, except on leave of absence, for 3 consecutive meetings of the board; or

(e) if the member engages in paid work that, in the opinion of the responsible Ministers, conflicts or could conflict with the proper performance of the member's duties.

113 Trusted digital identity advisory board members—other terms and conditions

A member of the trusted digital identity advisory board holds office on the terms and conditions (if any), in relation to matters not covered by this Act, that are determined by the Minister.

114 Trusted digital identity advisory board procedures

(1) The trusted digital identity advisory board is to hold any meetings necessary for the performance of its functions, and must meet at least twice every calendar year.

(2) Meetings of the trusted digital identity advisory board may be convened by the Minister.

(3) Except as mentioned in this section, the trusted digital identity advisory board is to determine its own procedures.

115 Advisory committees

(1) The Minister may establish, in writing, such advisory committees as the Minister considers appropriate to provide advice to the Oversight Authority in relation to the performance of the Oversight Authority's functions and exercise of the Authority's powers.

(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 7—Administration

Part 1—Introduction

116 Simplified outline of this Chapter

Part 2—Registers

117 TDIF accredited entities register

(1) The Oversight Authority must establish and maintain a register (the ***TDIF accredited entities register***) of entities who are, or have been, accredited entities.

(2) The TDIF 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 of accreditation imposed under subsection 52(2) that are in force, including any variations to those conditions, and the day the condition or variation took effect;

(c) any conditions of accreditation imposed under subsection 52(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) any other information prescribed by the TDI rules.

(3) Despite subsection (2), the TDIF accredited entities register must not contain details about an entity if:

(a) the entity is or was accredited as a particular kind of accredited entity; and

(b) the entity holds or held an approval to onboard to the trusted digital identity system as that kind of accredited entity.

Note: Information on these entities is held in the TDIS register.

(4) In subsection (3):

(a) a reference to an entity that is accredited includes a reference to an entity whose accreditation is suspended; and

(b) a reference to an entity that holds an approval includes a reference to an entity whose approval is suspended.

(5) The TDIF accredited entities register may contain any other information that the Oversight Authority considers appropriate.

(6) 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 Oversight Authority must remove the entity from the TDIF accredited entities register at the end of that period.

(7) The TDI rules may make provision for and in relation to the following:

(a) the correction of information in the TDIF accredited entities register;

(b) any other matter relating to the administration or operation of the TDIF accredited entities register.

(8) The TDIF accredited entities register must be made publicly available on the Oversight Authority's website.

(9) The TDIF accredited entities register is not a legislative instrument.

118 TDIS register

(1) The Oversight Authority must establish and maintain a register (the ***TDIS register***) of entities who have onboarded to the trusted digital identity system.

(2) The TDIS register must contain the following details for each entity:

(a) the day the entity's approval to onboard to the trusted digital identity system came into force;

(b) the entity's onboarding 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 trusted digital identity system;

(ii) if the participating relying party provides, or may provide, attributes of individuals obtained from the trusted digital identity system to other relying parties—details of those relying parties, including the services they provide or provide access to;

(d) any conditions on onboarding imposed under subsection 22(4) that are in force, including any variations to those conditions, and the day the condition or variation took effect;

(e) any conditions on onboarding imposed under subsection 22(4) that have been revoked, and the day the revocation took effect;

(f) if the entity's approval to onboard is or has been suspended for a period—that fact and the period of the suspension;

(g) if the entity's approval to onboard is or has been suspended until a specified event occurs or action is taken—that fact and the event or action;

(h) if the entity's approval to onboard is or has been suspended indefinitely—that fact;

(i) any exemptions from the interoperability obligation granted to the entity;

(j) any other information prescribed by the TDI rules.

(3) The TDIS register may contain any other information that the Oversight Authority considers appropriate.

(4) If an entity's approval to onboard to the trusted digital identity system is revoked, and the entity does not hold another approval to onboard to the trusted digital identity system for 3 years after the day the revocation came into force, the Oversight Authority must remove the entity from the TDIS register at the end of that period.

(5) The TDI rules may make provision for and in relation to the following:

(a) the correction of information in the TDIS register;

(b) any other matter relating to the administration or operation of the TDIS register.

(6) The TDIS register must be made publicly available on the Oversight Authority's website.

(7) The TDIS register is not a legislative instrument.

Part 3—Compliance and enforcement

Division 1—Powers of investigation and enforcement

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 is an authorised applicant in relation to the civil penalty provisions in Division 2 of Part 2 of Chapter 4 of this Act (about additional privacy safeguards); and

(b) the Oversight Authority 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.

Infringement officer

(2) For the purposes of Part 5 of the Regulatory Powers Act, the Oversight Authority is an infringement officer in relation to the provisions mentioned in subsection (1).

Relevant chief executive

(3) For the purposes of Part 5 of the Regulatory Powers Act, the Oversight Authority is the relevant chief executive in relation to the provisions mentioned in subsection (1).

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 4 of this Act (about additional privacy safeguards); and

(b) the Oversight Authority 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.

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 4 of this Act (about additional privacy safeguards); and

(b) the Oversight Authority 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 Oversight Authority's power to give directions to entities in relation to onboarding and accreditation

(1) The Oversight Authority 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 Oversight Authority considers it necessary to:

(a) give effect to a decision to approve an entity to onboard to the trusted digital identity system; or

(b) give effect to a decision to suspend or revoke an entity's approval to onboard to the trusted identity system; or

(c) to deal with matters arising as a result of the suspension or revocation of an entity's approval to onboard to the trusted identity 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 to:

(i) provide information to an entity that holds an approval to onboard to the trusted digital identity system about the steps required to connect to the system; and

(ii) to connect the entity to the trusted digital identity system by a specified date; or

(b) require an entity whose accreditation has been suspended or revoked to notify other participants in the digital identity 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 Oversight Authority's power to give directions to protect the integrity or performance of the trusted digital identity system

(1) The Oversight Authority may give a direction to the following entities if the Oversight Authority considers it necessary to do so to protect the integrity or performance of the trusted digital identity system:
  (a) entities that hold an approval to onboard to the trusted digital identity system;
  (b) entities whose approval to onboard to the trusted digital identity system is suspended;
  (c) accredited entities;
  (d) entities whose accreditation as an accredited entity is suspended.

(2) Without limiting subsection (1), the Oversight Authority 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 Oversight Authority;
  (b) conduct a fraud assessment in relation to a specified matter and provide a report to the Oversight Authority in relation to the assessment;
  (c) conduct a security assessment in relation to a specified matter and provide a report to the Oversight Authority in relation to the assessment;
  (d) an act or thing specified by the TDI rules.

(3) If TDIF accreditation rules made for the purposes of paragraph 59(2)(b) 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 Oversight Authority 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 Oversight Authority 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 Oversight Authority may, by written notice, require an entity to arrange for an assessment (a ***compliance assessment***) to be conducted:

(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 Oversight Authority 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 identity fraud incident;

(iii) a serious or repeated breach of the TDIF accreditation rules;

(iv) an incident that is having, or may have, a material impact on the operation of the entity's accredited facility;

(v) an incident that is having, or may have, a material impact on the operation of the trusted digital identity 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) circumstances specified in the TDI rules exist in relation to an entity.

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 entity must arrange for the compliance assessment to be undertaken; and

(b) whether the compliance assessment must be undertaken by:

(i) the Oversight Authority; or

(ii) an approved assessor.

(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 onboard to the trusted digital identity system and is given a notice under subsection (1), the Oversight Authority is not required to make a decision on the application until the assessment is conducted (see subsection 139(4)).

Note 2: For accredited entities and entities that hold an approval to onboard to the trusted digital identity 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 TDI rules may make provision for and in relation to compliance assessments.

(5) Without limiting subsection (4), the TDI rules may make provision for or in relation to the following:

(a) the functions to be performed, or the powers to be exercised, by persons conducting compliance assessments;

(b) processes to be followed during a compliance assessment or after a compliance assessment has been conducted;

(c) information that must be provided to or by an entity during a compliance assessment or after a compliance assessment has been conducted;

(d) requirements in relation to reports to be provided in relation to a compliance assessment;

(e) actions the Oversight Authority may require the entity subject to a compliance assessment to take after the assessment has been conducted.

(6) This section does not limit the TDIF accreditation rules that may be made for the purposes of paragraph 59(2)(c).

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.

128 Approved assessors

(1) The Oversight Authority may, in writing, approve a person to be an approved assessor for the purposes of this Act.

(2) An approval given under subsection (1) is not a legislative instrument.

(3) The Oversight Authority may publish, on the Oversight Authority's website, a list of approved assessors.

(4) The TDI rules may make provision for matters relating to the approval of persons under subsection (1).

(5) Without limiting subsection (4), the TDI rules may make provision for and in relation to the following:

(a) applications for approval;
(b) dealing with such applications;
(c) requirements that must be met for approval;
(d) matters to which the Oversight Authority may or must have regard in considering an application for approval;
(e) conditions of an approval;
(f) the period of effect of an approval;
(g) suspension and revocation of approvals.

129 Approved assessors may charge fees

(1) An approved assessor may charge a fee in relation to things done in the performance of the approved assessor's functions under this Act.

(2) A fee must not be such as to amount to taxation.

Division 4—Power to require information or documents

130 Power to require information or documents

(1) This section applies if the Oversight Authority 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 Oversight Authority's functions, or the exercise of any of the Oversight Authority's powers, under this Act.

(2) The Oversight Authority may, by written notice, require the entity:

(a) to give to the Oversight Authority, within the period and in the manner and form specified in the notice, any such information; or

(b) to produce to the Oversight Authority, 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 shorter 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.

Part 4—Record keeping

131 Record keeping by onboarded entities and former onboarded entities

(1) This section applies to:

(a) entities that hold an approval to onboard to the trusted digital identity system; and

(b) entities whose approval to onboard to the trusted digital identity system is suspended; and

(c) entities whose approval to onboard to the trusted digital identity 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 TDI rules.

Civil penalty: 200 penalty units.

(4) TDI 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 trusted digital identity 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.

132 Destruction or de-identification of certain information

(1) This section applies to:

(a) accredited entities that hold an approval to onboard to the trusted digital identity system; and

(b) accredited entities whose approval to onboard to the trusted digital identity system is suspended; and

(c) accredited entities whose approval to onboard to the trusted digital identity system has been revoked.

(2) The accredited entity must destroy or de-identify information held by the entity if the information:

(a) is personal information; and

(b) was obtained by the entity through the trusted digital identity system; and

(c) the entity is not required 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 TDI rules made for the purposes of section 131.

Civil penalty: 200 penalty units.

Part 5—Review of decisions

133 Reviewable decisions

(1) A decision by the Oversight Authority 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 *Reviewable decision*	Column 2 *Affected entity*
1	A decision under section 18 to refuse to approve an entity to onboard to the trusted digital identity system	The entity who made the application
2	A decision under subsection 20(1) to direct the Oversight Authority to refuse to approve an entity to onboard to the trusted digital identity system	The entity subject to the direction
3	A decision under subsection 20(2) to direct the Oversight Authority to suspend an entity's approval to onboard to the trusted digital identity system	The entity subject to the direction
4	A decision under subsection 22(4) to impose conditions on an entity's approval to onboard to the trusted digital identity system	The entity on whom the conditions are imposed
5	A decision under subsection 24(1) to vary, on the Oversight Authority's own initiative, the conditions imposed on an entity's approval to onboard to the trusted digital	The entity on whom the conditions are imposed

Section 133

Reviewable decisions		
Item	**Column 1** ***Reviewable decision***	**Column 2** ***Affected entity***
	identity system	
6	A decision under subsection 24(1) to refuse to vary, on application by an entity, the conditions imposed on the entity's approval to onboard to the trusted digital identity system	The entity who made the application
7	A decision under subsection 28(2) to suspend an entity's approval to onboard to the trusted digital identity system	The entity that holds the approval
8	A decision under subsection 28(3) to refuse to suspend, on application by an entity, the entity's approval to onboard to the trusted digital identity system	The entity who made the application
9	A decision under subsection 28(9) or (10) to refuse to revoke a suspension of an entity's approval to onboard to the trusted digital identity system	The entity whose approval is suspended
10	A decision under subsection 29(1) to revoke an entity's approval to onboard to the trusted digital identity system	The entity that held the approval
11	A decision under subsection 30(3) to refuse to grant an exemption to a participating relying party	The participating relying party who made the application
12	A decision under section 34 to refuse to grant an exemption from the interoperability obligation to an entity	The entity who made the application
13	A decision under section 48 to refuse to grant an authorisation to an entity to apply for accreditation	The entity who made the application
14	A decision under section 50 to	The entity who made the application

Reviewable decisions		
Item	**Column 1** ***Reviewable decision***	**Column 2** ***Affected entity***
	refuse to accredit an entity as an accredited entity	
15	A decision under subsection 52(2) to impose conditions on an entity's accreditation	The entity on whom the conditions are imposed
16	A decision under subsection 53(1) to vary, on the Oversight Authority's own initiative, the conditions imposed on an entity's accreditation	The entity on whom the conditions are imposed
17	A decision under subsection 53(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
18	A decision under subsection 57(1) to suspend the accreditation of an accredited entity	The accredited entity
19	A decision under subsection 58(1) to revoke an entity's accreditation	The entity whose accreditation is revoked
20	A decision under subsection 58(2) to refuse to revoke, on application by an entity, an entity's accreditation	The entity who made the application
21	A decision to give a direction to an entity under Division 2 of Part 3 of Chapter 7	The entity subject to the direction

(2) The TDI 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 entity ***affected*** by the reviewable decision.

(3) 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***.

134 Internal review—decisions made by delegates of the Oversight Authority

(1) If an entity is affected by a reviewable decision made by a delegate of the Oversight Authority, the entity may apply in writing to the Oversight Authority 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.

135 Reconsideration by Oversight Authority

(1) Within 90 days after receiving an application under section 134 for internal review, the Oversight Authority must:

(a) review the decision; and

(b) affirm, vary or revoke the decision; and

(c) if the Oversight Authority revokes the decision—make such other decision (if any) that the Oversight Authority thinks appropriate.

(2) The Oversight Authority must, as soon as practicable after making a decision under subsection (1), give the applicant a written statement of the Oversight Authority's reasons for the decision.

(3) If the Oversight Authority's functions under this section are performed by a delegate of the Oversight Authority, 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.

136 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 Oversight Authority personally;

(b) an internal review decision made by the Oversight Authority under subsection 135(1).

(2) An application under subsection (1) may be made only by, or on behalf of, an entity affected by the reviewable decision.

(3) Subsection (2) has effect despite subsection 27(1) of the *Administrative Appeals Tribunal Act 1975*.

Part 6—Applications under this Act

137 Requirements for applications

(1) An application made under this Act to the Oversight Authority must:

(a) be given in a form and manner approved by the Oversight Authority for that kind of application; and

(b) be accompanied by any information or documents required by the form; and

(c) if TDI rules made for the purposes of section 140 specify a fee that must accompany the application and payment of the fee has not been waived—be accompanied by the fee.

Note: The Oversight Authority is not required to make a decision on the application if this subsection is not complied with (see section 139).

(2) The Oversight Authority may accept any information or document previously given to the Oversight Authority 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, the Oversight Authority may approve:

(a) different forms for different kinds of applications; or

(b) a single form for more than one kind of application.

138 Powers of Oversight Authority in relation to applications

(1) This section applies if an application is made under this Act to the Oversight Authority.

(2) The Oversight Authority may, by written notice, require an applicant to give the Oversight Authority such further information or documents in relation to the application as the Oversight Authority reasonably requires.

Note 1: The Oversight Authority may also require an applicant to undergo a compliance assessment before making a decision on the application (see section 126).

Note 2: The Oversight Authority is not required to make a decision on the application if this subsection is not complied with (see section 139).

(3) A notice under subsection (2) may specify a period, which must not be less than 14 days, within which the information or documents must be given.

139 Oversight Authority not required to make a decision in certain circumstances

(1) If this Act requires an application to be in a form approved by the Oversight Authority, the Oversight Authority 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 Oversight Authority is not required to make a decision on the application until the information or documents are provided.

(3) If this Act permits the Oversight Authority to require further information or documents in relation to an application, the Oversight Authority is not required to make a decision on the application until the information or documents are provided.

(4) If this Act permits the Oversight Authority to require a compliance assessment to be conducted for the purposes of making a decision, the Oversight Authority is not required to make the decision until the assessment is conducted.

(5) If TDI rules made for the purposes of section 140 specify a fee that must accompany an application and payment of the fee has not been waived, the Oversight Authority is not required to make a decision on the application until the fee is paid.

Part 7—Fees

Division 1—Fees charged by the Oversight Authority

140 Charging of fees by Oversight Authority

(1) The TDI rules may make provision in relation to the charging of fees by the Oversight Authority for activities carried out by or on behalf of the Oversight Authority in performing functions or exercising powers under this Act.

(2) Without limiting subsection (1), the TDI 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 Oversight Authority 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 TDI 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 identity of the individual.

(4) A fee prescribed by the TDI 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 TDI 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 TDI rules may provide for the extension of any times for providing services accordingly.

141 Review of fees

(1) The Minister must cause periodic reviews of rules made for the purposes of subsection 140(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 Oversight Authority's website.

142 Recovery of fees charged by the Oversight Authority

A fee 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.

143 Commonwealth not liable to pay fees charged by the Oversight Authority

(1) The Commonwealth is not liable to pay a fee that is payable under this Act. 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 Commonwealth law.

(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 Commonwealth law.

Division 2—Fees charged by accredited entities

144 Charging of fees by accredited entities in relation to the trusted digital identity system

(1) An accredited entity that charges fees in relation to the services it provides in relation to the trusted digital identity system must do so in accordance with the TDI rules (if any) made for the purposes of subsection (2).

(2) The TDI rules may make provision in relation to the charging of fees by accredited entities for services provided in relation to trusted digital identity system.

(3) Without limiting subsection (2), the TDI 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 services it provides, either in relation to the trusted digital identity system or otherwise.

Chapter 8—Other matters

145 Simplified outline of this Chapter

146 Annual report by Oversight Authority

(1) After the end of each financial year, the Oversight Authority must prepare and give a report to the Minister, for presentation to the Parliament, on the Oversight Authority's activities during the financial year.

(2) The report must include the following:

(a) information about the operation of the trusted digital identity system, including:

(i) the number of applications made to onboard to the system under section 16; and

(ii) the number of approvals granted to onboard to the system under section 18; and

(iii) the number of digital identity fraud incidents or cyber security incidents, and the responses to any such incidents;

(b) information about the operation of the accreditation scheme, including:

(i) the number of applications for accreditation made under section 49; and

(ii) the number of accreditations granted under section 50;

(c) information on any other matters notified by the Minister to the Oversight Authority.

(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*.

147 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 4 of this Act during the period.

148 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.

149 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 or body, 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).

150 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).

151 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.

152 Protection from civil action

(1) This section applies to:
(a) the Oversight Authority; and
(b) a person whose services are made available to the Oversight Authority under section 100; and
(c) a person engaged by the Oversight Authority under section 101 or 102.

(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.

153 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 at least one of the following paragraphs applies in relation to the conduct constituting the alleged contravention:
(a) the conduct occurs wholly or partly in Australia, or wholly or partly on board an Australian aircraft or Australian ship;
(b) for conduct alleged to constitute an ancillary contravention:
(i) the conduct occurs wholly outside Australia; and
(ii) the conduct that would constitute the primary contravention to which the ancillary contravention relates would have occurred wholly or partly in

Australia or wholly or partly on board an Australian aircraft or an Australian ship;

(c) the conduct occurs wholly outside Australia and the entity engaging in the conduct is an Australian entity.

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 primary contravention to which the alleged contravention relates occurs, or would have occurred, 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 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.

(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.

(5) 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

(6) 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.

154 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.

155 Delegation—Minister

(1) The Minister may, in writing, delegate all or any of the Minister's functions or powers under this Act to any of the following:

(a) the Oversight Authority;

(b) the Secretary of the Department;

(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.

156 Delegation—Oversight Authority

(1) The Oversight Authority may, in writing, delegate all or any of the Oversight Authority's powers or functions under this Act to a member of the staff assisting the Oversight Authority as mentioned in subsection 100(1) who is:

(a) an SES employee, or acting SES employee; or

(b) an APS employee who holds or is acting in an Executive Level 2, or equivalent, position.

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 Oversight Authority.

157 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 Oversight Authority 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 the rules.

158 Rules—requirement to consult

General requirement to consult

(1) Before making or amending any rules under section 157, 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 28 days after the notice is published; and

(b) consider any submissions received within the 28-day period.

Exception if imminent threat etc.

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

(a) the Minister is satisfied that there is an imminent threat to the trusted digital identity system; or

(b) the Minister is satisfied that a hazard has had, or is having, a significant impact on the trusted digital identity system.

Review

(3) If, because of subsection (2), subsection (1) did not apply to the making of rules or amendments, the Secretary must:

(a) review the operation, effectiveness and implications of the rules or amendments; and

(b) without limiting paragraph (a), consider whether any amendments should be made; and

(c) give the Minister a report of the review and a statement setting out the Secretary's findings.

(4) 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 28 days after the notice is published; and

(b) consider any submissions received within the 28-day period mentioned in paragraph (a).

Findings of review to be tabled

(5) The Secretary must complete the review within 60 days after the commencement of the rules or amendments concerned.

(6) 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.

(7) 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

(8) This section does not limit section 17 of the *Legislation Act 2003* (rule-makers should consult before making legislative instrument).