

# EXPOSURE DRAFT

2022-2023

The Parliament of the  
Commonwealth of Australia

HOUSE OF REPRESENTATIVES/THE SENATE

EXPOSURE DRAFT

## **Digital ID Bill 2023**

**No. , 2023**

*(Finance)*

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

EXPOSURE DRAFT



# EXPOSURE DRAFT

---

## Contents

<b>Chapter 1—Introduction</b>	2
<b>Part 1—Preliminary</b>	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
<b>Part 2—Interpretation</b>	5
9	Definitions.....5
10	Meaning of <i>attribute</i> of an individual.....13
11	Meaning of <i>restricted attribute</i> of an individual.....14
12	Fit and proper person considerations .....15
<b>Chapter 2—Accreditation</b>	16
<b>Part 1—Introduction</b>	16
13	Simplified outline of this Chapter .....16
<b>Part 2—Accreditation</b>	17
<b>Division 1—Applying for accreditation</b>	17
14	Application for accreditation .....17
<b>Division 2—Accreditation</b>	18
15	Digital ID Regulator must decide whether to accredit an entity .....18
16	Minister’s directions regarding accreditation .....20
17	Accreditation is subject to conditions.....20
18	Conditions on accreditation .....21
19	Requirements before Accreditation Rules impose conditions relating to restricted attributes or biometric information of individuals .....22
20	Variation and revocation of conditions on accreditation .....23
21	Applying for variation or revocation of conditions on accreditation .....23

# EXPOSURE DRAFT

---

22	Notice before changes to conditions on accreditation .....	24
23	Notice of decision of changes to conditions on accreditation .....	25
<b>Division 3—Varying, suspending and revoking accreditation</b>		26
24	Varying accreditation .....	26
25	Suspension of accreditation .....	26
26	Revocation of accreditation .....	29
<b>Division 4—Accreditation Rules</b>		32
27	Accreditation Rules .....	32
<b>Division 5—Other matters relating to accredited entities</b>		34
28	Digital IDs must be deactivated on request .....	34
29	Accredited services must be accessible and inclusive .....	34
<b>Chapter 3—Privacy</b>		35
<b>Part 1—Introduction</b>		35
30	Simplified outline of this Chapter .....	35
31	Chapter applies to accredited entities only to the extent the entity is providing accredited services etc. ....	35
32	APP-equivalent agreements.....	35
<b>Part 2—Privacy</b>		36
<b>Division 1—Interaction with the Privacy Act 1988</b>		36
33	Extended meaning of <i>personal information</i> in relation to accredited entities .....	36
34	Privacy obligations for non-APP entities .....	36
35	Contraventions of privacy obligations in APP-equivalent agreements.....	37
36	Contraventions of Division 2 are interferences with privacy.....	38
37	Notification of eligible data breaches—accredited entities that are APP entities .....	39
38	Notification of eligible data breaches—accredited entities that are not APP entities.....	39
39	Notification of corresponding data breaches—accredited State or Territory entities that are not APP entities.....	40

# EXPOSURE DRAFT

---

40	Additional function of the Information Commissioner .....	40
<b>Division 2—Additional privacy safeguards</b>		42
41	Collection etc. of certain attributes of individuals is prohibited.....	42
42	Individuals must expressly consent to disclosure of certain attributes of individuals to relying parties.....	42
43	Disclosure of restricted attributes of individuals .....	43
44	Restricting the disclosure of unique identifiers .....	43
45	Restrictions on collecting, using and disclosing biometric information.....	45
46	Authorised collection, use and disclosure of biometric information of individuals—general rules.....	45
47	Accredited identity service providers may collect etc. biometric information for purposes of government identity documents.....	48
48	Destruction of biometric information of individuals .....	49
49	Other rules relating to biometric information .....	50
50	Data profiling to track online behaviour is prohibited .....	51
51	Personal information must not be used or disclosed for prohibited enforcement purposes .....	51
52	Personal information must not be used or disclosed for prohibited marketing purposes.....	53
53	Accredited identity exchange providers must not retain certain attributes of individuals .....	53
<b>Chapter 4—The Australian Government Digital ID System</b>		55
<b>Part 1—Introduction</b>		55
54	Simplified outline of this Chapter .....	55
<b>Part 2—The Australian Government Digital ID System</b>		56
<b>Division 1—The Australian Government Digital ID System</b>		56
55	Digital ID Regulator must oversee and maintain the Australian Government Digital ID System.....	56
56	Circumstances in which entities may provide or receive services within the Australian Government Digital ID System.....	56

# EXPOSURE DRAFT

---

<b>Division 2—Participating in the Australian Government Digital ID System</b>	60
57 Phasing-in of participation in the Australian Government Digital ID System .....	60
58 Applying for approval to participate in the Australian Government Digital ID System.....	60
59 Approval to participate in the Australian Government Digital ID System .....	61
60 Minister’s directions regarding participation.....	63
61 Approval to participate in the Australian Government Digital ID System is subject to conditions .....	63
62 Conditions on approval to participate in the Australian Government Digital ID System.....	64
63 Conditions relating to restricted attributes of individuals .....	66
64 Variation and revocation of conditions.....	68
65 Applying for variation or revocation of conditions on approval .....	69
66 Notice before changes to conditions on approval .....	69
67 Notice of decision of changes of conditions on approval.....	70
<b>Division 3—Varying, suspending and revoking approval to participate</b>	71
68 Varying approval to participate in the Australian Government Digital ID System .....	71
69 Suspension of approval to participate in the Australian Government Digital ID System.....	71
70 Revocation of approval to participate in the Australian Government Digital ID System.....	74
<b>Division 4—Other matters relating to the Australian Government Digital ID System</b>	77
71 Creating and using a digital ID is voluntary .....	77
72 Notice before exemption is revoked .....	79
73 Holding etc. information outside Australia.....	79
74 Reportable incidents .....	80
75 Interoperability .....	81
76 Service levels for accredited entities and participating relying parties .....	83
77 Entities may conduct testing in relation to the Australian Government Digital ID System.....	83

---

# EXPOSURE DRAFT

---

78	Use and disclosure of personal information to conduct testing.....	84
<b>Part 3—Liability and redress framework</b>		85
<b>Division 1—Liability of participating entities</b>		85
79	Accredited entities participating in the Australian Government Digital ID System protected from liability in certain circumstances .....	85
<b>Division 2—Statutory contract</b>		86
80	Statutory contract between entities participating in the Australian Government Digital ID System.....	86
81	Participating entities to maintain insurance as directed by Digital ID Regulator .....	87
82	Dispute resolution procedures .....	88
<b>Division 3—Redress framework</b>		89
83	Redress framework.....	89
<b>Chapter 5—Digital ID Regulator</b>		90
<b>Part 1—Introduction</b>		90
84	Simplified outline of this Chapter .....	90
<b>Part 2—Digital ID Regulator</b>		91
85	Digital ID Regulator.....	91
86	Functions of the Digital ID Regulator .....	91
87	Powers of the Digital ID Regulator .....	92
<b>Division 2—Confidentiality obligations of the Digital ID Regulator and certain other persons</b>		93
88	Prohibition on entrusted persons using or disclosing personal or commercially sensitive information .....	93
89	Authorised uses and disclosures of personal or commercially sensitive information by entrusted persons .....	94
90	Disclosing personal or commercially sensitive information to courts and tribunals etc. by entrusted persons .....	95
<b>Part 2—Advisory committees</b>		96
91	Advisory committees.....	96
<b>Chapter 6—Digital ID Data Standards</b>		97

---

# EXPOSURE DRAFT

---

<b>Part 1—Introduction</b>	97
92	Simplified outline of this Chapter ..... 97
<b>Part 2—Digital ID Data Standards</b>	98
93	Digital ID Data Standards ..... 98
94	Requirement to consult before making..... 98
<b>Part 3—Digital ID Data Standards Chair</b>	100
<b>Division 1—Establishment and functions of the Digital ID Data Standards Chair</b>	100
95	Data Standards Chair ..... 100
96	Functions of the Digital ID Data Standards Chair ..... 100
97	Powers of the Digital ID Data Standards Chair ..... 100
98	Directions to the Digital ID Data Standards Chair ..... 100
<b>Division 2—Appointment of the Digital ID Data Standards Chair</b>	101
99	Appointment ..... 101
100	Term of appointment ..... 101
101	Acting appointments..... 101
102	Application of the finance law etc. .... 102
<b>Division 3—Terms and conditions for the Digital ID Data Standards Chair</b>	103
103	Remuneration ..... 103
104	Leave of absence ..... 103
105	Outside work ..... 104
106	Disclosure of interests ..... 104
107	Resignation of appointment..... 104
108	Termination of appointment ..... 105
109	Other terms and conditions..... 105
<b>Division 4—Other matters</b>	106
110	Arrangements relating to staff ..... 106
111	Consultants ..... 106
<b>Chapter 7—Trustmarks and registers</b>	107
<b>Part 1—Introduction</b>	107
112	Simplified outline of this Chapter ..... 107
<b>Part 2—Digital ID trustmarks</b>	108
113	Digital ID trustmarks ..... 108

---



# EXPOSURE DRAFT

---

114	Authorised use of digital ID trustmarks etc. ....	108
115	Displaying digital ID trustmark .....	109
<b>Part 3—Registers</b>		<b>110</b>
116	Digital ID Accredited Entities Register .....	110
117	AGDIS Register .....	111
<b>Chapter 8—Administration</b>		<b>114</b>
<b>Part 1—Introduction</b>		<b>114</b>
118	Simplified outline of this Chapter .....	114
<b>Part 2—Compliance and enforcement</b>		<b>115</b>
<b>Division 1—Enforcement powers</b>		<b>115</b>
119	Civil penalty provisions.....	115
120	Infringement notices.....	116
121	Enforceable undertakings .....	116
122	Injunctions.....	117
<b>Division 2—Directions powers</b>		<b>119</b>
123	Digital ID Regulator’s power to give directions to entities in relation to participation and accreditation .....	119
124	Digital ID Regulator’s power to give directions to protect the integrity or performance of the Australian Government Digital ID System.....	120
125	Remedial directions to accredited entities etc.....	121
<b>Division 3—Compliance assessments</b>		<b>122</b>
126	Compliance assessments .....	122
127	Entities must provide assistance to persons undertaking compliance assessments .....	123
<b>Division 4—Power to require information or documents</b>		<b>124</b>
128	Power to require information or documents .....	124
<b>Part 3—Record keeping</b>		<b>125</b>
129	Record keeping by participating entities and former participating entities .....	125
130	Destruction or de-identification of certain information .....	125
<b>Part 4—Review of decisions</b>		<b>127</b>
131	Reviewable decisions .....	127

---

# EXPOSURE DRAFT

---

132	Internal review of decisions made by delegates of the Digital ID Regulator .....	130
133	Reconsideration by Digital ID Regulator .....	130
134	Review by the Administrative Appeals Tribunal.....	131
<b>Part 5—Applications under this Act</b>		132
135	Requirements for applications .....	132
136	Powers in relation to applications.....	132
137	Decisions not required to be made in certain circumstances .....	133
<b>Part 6—Fees</b>		134
<b>Division 1—Fees charged by the Digital ID Regulator</b>		134
138	Charging of fees by Digital ID Regulator etc. ....	134
139	Review of fees .....	135
140	Recovery of fees charged by the Digital ID Regulator .....	135
141	Commonwealth not liable to pay fees charged by entities that are part of the Commonwealth .....	135
<b>Division 2—Fees charged by accredited entities</b>		137
142	Charging of fees by accredited entities in relation to the Australian Government Digital ID System .....	137
<b>Chapter 9—Other matters</b>		138
143	Simplified outline of this Chapter .....	138
144	Annual report by Digital ID Regulator .....	138
145	Annual report by Information Commissioner.....	139
146	Treatment of partnerships.....	139
147	Treatment of unincorporated associations .....	139
148	Treatment of trusts .....	140
149	Treatment of certain Commonwealth, State and Territory entities .....	141
150	Bodies corporate and due diligence .....	143
151	Protection from civil action .....	143
152	Geographical jurisdiction of civil penalty provisions .....	144
153	Review of operation of Act .....	146
154	Delegation—Minister .....	147
155	Delegation—Digital ID Regulator.....	147
156	Delegation—Digital ID Data Standards Chair .....	148

# EXPOSURE DRAFT

---

157	Instruments may incorporate etc. material as in force or existing from time to time .....	148
158	Rules—general matters .....	149
159	Rules—requirement to consult .....	150



# EXPOSURE DRAFT

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

5 The Parliament of Australia enacts:

EXPOSURE DRAFT

# EXPOSURE DRAFT

Chapter 1 Introduction

Part 1 Preliminary

Section 1

---

1 **Chapter 1—Introduction**

2 **Part 1—Preliminary**

3

4 **1 Short title**

5 This Act is the *Digital ID Act 2023*.

6 **2 Commencement**

7 (1) Each provision of this Act specified in column 1 of the table  
8 commences, or is taken to have commenced, in accordance with  
9 column 2 of the table. Any other statement in column 2 has effect  
10 according to its terms.

11

---

**Commencement information**

---

<b>Column 1</b>	<b>Column 2</b>	<b>Column 3</b>
<b>Provisions</b>	<b>Commencement</b>	<b>Date/Details</b>

---

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.	
-------------------------	---	--

---

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

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

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

## 3 Objects

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33

- (1) The objects of this Act are as follows:
  - (a) to provide individuals with a simple, inclusive and convenient method for verifying their identity in online transactions with government and businesses, while protecting their privacy and the security of their personal information;
  - (b) to promote economic advancement by building trust in digital ID services;
  - (c) to facilitate economic benefits for, and reduce burdens on, the Australian economy by encouraging the use of digital IDs and online services;
  - (d) to provide a digital ID system that will enable innovative digital sectors of the Australian economy to flourish.
  
- (2) These objects are to be achieved by:
  - (a) enhancing the simplicity, safety, privacy and security of online transactions between individuals, government and businesses by:
    - (i) establishing a system of voluntary accreditation for entities participating in digital ID systems other than the Australian Government Digital ID System, ensuring such entities comply with the same strong privacy and integrity safeguards as those that apply to the Australian Government Digital ID System; and
    - (ii) improving the regulation and governance of providers of services within such systems; and
  - (b) establishing an Australian Government Digital ID System that is safe, secure, trusted, accessible, inclusive, easy to use, reliable and voluntary, and supported by strong privacy and integrity safeguards; and
  - (c) facilitating choice for individuals amongst providers of services within the Australian Government Digital ID System.

# EXPOSURE DRAFT

Chapter 1 Introduction

Part 1 Preliminary

Section 4

---

1 **4 Simplified outline of this Act**

2

[to be drafted]

3 **5 Act binds the Crown**

4

This Act binds the Crown in each of its capacities.

5 **6 Extension to external Territories**

6

This Act extends to every external Territory.

7 **7 Extraterritorial operation**

8

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

9

10

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

11

12

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

13

14

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

15

16

17

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

18

19 **8 Concurrent operation of State and Territory laws**

20

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.

21

22



## Part 2—Interpretation

### 9 Definitions

In this Act:

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

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

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

- (a) an accredited attribute service provider;
- (b) an accredited identity exchange provider;
- (c) an accredited identity service provider;
- (d) if Accreditation Rules are made for the purposes of paragraph 14(1)(d)—an entity that is accredited to provide services of a kind prescribed by the Accreditation Rules for the purposes of that paragraph.

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

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

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

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

# EXPOSURE DRAFT

## Chapter 1 Introduction

## Part 2 Interpretation

### Section 9

---

1                   Example: Acme Co is an accredited identity service provider. Under its  
2                   conditions of accreditation, its accredited service is generating,  
3                   managing, maintaining and verifying information relating to the  
4                   identity of an individual. Its conditions exclude from its accreditation  
5                   the provision of the following services:  
6                   (a) generating, binding, managing and distributing authenticators to  
7                   an individual;  
8                   (b) binding, managing and distributing authenticators generated by  
9                   an individual.

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

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

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

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

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

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

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

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

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

- 25                   (a) an Australian citizen or a permanent resident of Australia;  
26                   (b) a body corporate incorporated by or under a law of the  
27                   Commonwealth or a State or Territory;  
28                   (c) a Commonwealth entity, or a Commonwealth company,  
29                   within the meaning of the *Public Governance, Performance*  
30                   *and Accountability Act 2013*;  
31                   (d) a person or body that is an agency within the meaning of the  
32                   *Freedom of Information Act 1982*;

# EXPOSURE DRAFT

## Section 9

---

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

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

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

12 Note: Passwords and cryptographic keys are examples of authenticators.

13 ***biometric information*** of an individual:

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

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

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

21 ***cyber security incident*** means one or more acts, events or  
22 circumstances that involve:

- 23 (a) unauthorised access to, modification of or interference with a  
24 system, service or network; or  
25 (b) an unauthorised attempt to gain access to, modify or interfere  
26 with a system, service or network; or  
27 (c) unauthorised impairment of the availability, reliability,  
28 security or operation of a system, service or network; or  
29 (d) an unauthorised attempt to impair the availability, reliability,  
30 security or operation of a system, service or network.

# EXPOSURE DRAFT

## Chapter 1 Introduction

## Part 2 Interpretation

### Section 9

---

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

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

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

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

- 9            (a) if a person holds an appointment under section 99—that  
10            person; or  
11            (b) otherwise—the Minister.

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

- 13           (a) occurs in connection with:  
14                (i) an accredited service of an accredited entity; or  
15                (ii) a service that a participating relying party is approved to  
16                provide, or provide access to, within the Australian  
17                Government Digital ID System; and  
18           (b) results in any of the following being, or suspected of being,  
19           compromised or rendered unreliable:  
20                (i) the digital ID of an individual;  
21                (ii) an attribute of an individual;  
22                (iii) an authenticator relating to an individual;  
23                (iv) a representation relating to an attribute of an individual;  
24                (v) a representation relating to a digital ID of an individual.

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

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

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

- 31           (a) the verification of the identity of individuals;

# EXPOSURE DRAFT

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

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

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

7 **enforcement body** has the same meaning as in the *Privacy Act*  
8 *1988*.

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

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

- 12 (a) an individual;
- 13 (b) a body corporate;
- 14 (c) a Commonwealth entity, or a Commonwealth company,  
15 within the meaning of the *Public Governance, Performance*  
16 *and Accountability Act 2013*;
- 17 (d) a person or body that is an agency within the meaning of the  
18 *Freedom of Information Act 1982*;
- 19 (e) a body specified, or the person holding an office specified, in  
20 Part I of Schedule 2 to the *Freedom of Information Act 1982*;
- 21 (f) a department or authority of a State;
- 22 (g) a department or authority of a Territory;
- 23 (h) a partnership;
- 24 (i) an unincorporated association;
- 25 (j) a trust.

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

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

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

# EXPOSURE DRAFT

## Chapter 1 Introduction

## Part 2 Interpretation

### Section 9

---

- 1 (a) generates, manages, maintains or verifies information  
2 relating to the identity of an individual; and  
3 (b) generates, binds, manages or distributes authenticators to an  
4 individual; and  
5 (c) binds, manages or distributes authenticators generated by an  
6 individual.

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

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

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

- 12 (a) the entity holds an approval under section 59 to participate in  
13 the system; and  
14 (b) either:  
15 (i) the entity is directly connected to an accredited entity  
16 that is participating in the Australian Government  
17 Digital ID System; or  
18 (ii) the entity is an accredited entity that is directly  
19 connected to a participating relying party.

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

- 22 (a) the relying party holds an approval under section 59 to  
23 participate in the Australian Government Digital ID System;  
24 and  
25 (b) the participation start day for the relying party has arrived or  
26 passed.

27 ***participation start day*** for an entity means the day notified to the  
28 entity by the Digital ID Regulator for the purposes of paragraph  
29 59(6)(c) as the day on which the entity must begin to participate in  
30 the Australian Government Digital ID System.

31 ***personal information***:

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

# EXPOSURE DRAFT

## Section 9

---

- 1 (i) whether the information or opinion is true or not; and  
2 (ii) whether the information or opinion is recorded in a  
3 material form or not; and  
4 (b) to the extent not already covered by paragraph (a), includes  
5 an attribute of an individual.

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

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

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

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

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

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

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

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

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

- 20 (a) subparagraph 15(5)(c)(ii);  
21 (b) subsection 16(1);  
22 (c) subsection 16(2);  
23 (d) subsection 18(4);  
24 (e) paragraph 20(2)(b);  
25 (f) paragraph 25(2)(d);  
26 (g) paragraph 26(1)(d);  
27 (h) paragraph 59(2)(a);  
28 (i) subsection 60(1);  
29 (j) subsection 60(2);  
30 (k) subsection 62(4);

# EXPOSURE DRAFT

## Chapter 1 Introduction

## Part 2 Interpretation

### Section 9

---

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

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

- 7 (a) the person has acquired or used an assumed identity under  
8 Part IAC of the *Crimes Act 1914* or a corresponding assumed  
9 identity law within the meaning of that Part;  
10 (b) an authority for the person to acquire or use an assumed  
11 identity has been granted under that Part or such a law;  
12 (c) a witness identity protection certificate has been given for the  
13 person under Part IACA of the *Crimes Act 1914*;  
14 (d) a corresponding witness identity protection certificate has  
15 been given for the person under a corresponding witness  
16 identity protection law within the meaning of Part IACA of  
17 the *Crimes Act 1914*;  
18 (e) the person is a participant as defined in the *Witness*  
19 *Protection Act 1994*;  
20 (f) the person is or was on a witness protection program  
21 conducted by a State or Territory in which a complementary  
22 witness protection law (as defined in the *Witness Protection*  
23 *Act 1994*) is in force;  
24 (g) the person is involved in administering such a program under  
25 such a law and the person has acquired an identity under that  
26 law.

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

31 **this Act** includes:

- 32 (a) the Accreditation Rules; and  
33 (b) the Digital ID Data Standards; and  
34 (c) the Digital ID Rules; and



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

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

## 6 **10 Meaning of *attribute* of an individual**

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

10 (2) Without limiting subsection (1), an **attribute** of an individual  
11 includes the following:

- 12 (a) the individual's current or former name;  
13 (b) the individual's current or former address;  
14 (c) the individual's date of birth;  
15 (d) information about whether the individual is alive or dead;  
16 (e) the individual's phone number;  
17 (f) the individual's email address;  
18 (g) if the individual has a digital ID—the time and date the  
19 digital ID was created;  
20 (h) biometric information of the individual;  
21 (i) a restricted attribute of the individual;  
22 (j) information or an opinion about the individual's:  
23 (i) racial or ethnic origin; or  
24 (ii) political opinions; or  
25 (iii) membership of a political association; or  
26 (iv) religious beliefs or affiliations; or  
27 (v) philosophical beliefs; or  
28 (vi) sexual orientation or practices.

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

# EXPOSURE DRAFT

## Chapter 1 Introduction

## Part 2 Interpretation

### Section 11

---

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

#### 4 **11 Meaning of *restricted attribute* of an individual**

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

- 6 (a) health information (within the meaning of the *Privacy Act*  
7 *1988*) about the individual; or  
8 (b) an identifier of the individual that has been issued or assigned  
9 by or on behalf of:  
10 (i) the Commonwealth, a State or a Territory; or  
11 (ii) an authority or agency of the Commonwealth, a State or  
12 a Territory; or  
13 (iii) a government of a foreign country; or  
14 (c) information or an opinion about the individual's criminal  
15 record; or  
16 (d) information or an opinion about the individual's membership  
17 of a professional or trade association;  
18 (e) information or an opinion about the individual's membership  
19 of a trade union;  
20 (f) other information or opinion that is associated with an  
21 individual and is prescribed by the Accreditation Rules.

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

- 24 (a) the individual's tax file number (within the meaning of  
25 section 202A of the *Income Tax Assessment Act 1936*);  
26 (b) the individual's medicare number (within the meaning of  
27 Part VII of the *National Health Act 1953*);  
28 (c) the individual's healthcare identifier (within the meaning of  
29 the *Healthcare Identifiers Act 2010*);  
30 (d) if the person holds a driver's licence issued under the law of  
31 a State or Territory—the number of that driver's licence.

# EXPOSURE DRAFT

1 **12 Fit and proper person considerations**

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

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

# EXPOSURE DRAFT

Chapter 2 Accreditation

Part 1 Introduction

Section 13

---

1 **Chapter 2—Accreditation**

2 **Part 1—Introduction**

3

4 **13 Simplified outline of this Chapter**

# EXPOSURE DRAFT

Accreditation **Chapter 2**  
Accreditation **Part 2**  
Applying for accreditation **Division 1**

Section 14

---

1 **Part 2—Accreditation**

2 **Division 1—Applying for accreditation**

3 **14 Application for accreditation**

- 4 (1) An entity covered by subsection (2) may apply to the Digital ID  
5 Regulator for accreditation as one of the following kinds of  
6 accredited entities:
- 7 (a) an accredited attribute service provider;
  - 8 (b) an accredited identity exchange provider;
  - 9 (c) an accredited identity service provider;
  - 10 (d) an entity that provides a service of a kind prescribed by the  
11 Accreditation Rules.

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

- 13 (2) An entity is covered by this section if the entity is one of the  
14 following:
- 15 (a) a body corporate incorporated by or under a law of the  
16 Commonwealth or a State or Territory;
  - 17 (b) a registered foreign company within the meaning of the  
18 *Corporations Act 2001*;
  - 19 (c) a Commonwealth entity, or a Commonwealth company,  
20 within the meaning of the *Public Governance, Performance*  
21 *and Accountability Act 2013*;
  - 22 (d) a person or body that is an agency within the meaning of the  
23 *Freedom of Information Act 1982*;
  - 24 (e) a body specified, or the person holding an office specified, in  
25 Part I of Schedule 2 to the *Freedom of Information Act 1982*;
  - 26 (f) a department or authority of a State;
  - 27 (g) a department or authority of a Territory.

# EXPOSURE DRAFT

Chapter 2 Accreditation

Part 2 Accreditation

Division 2 Accreditation

Section 15

---

1 **Division 2—Accreditation**

2 **15 Digital ID Regulator must decide whether to accredit an entity**

- 3 (1) This section applies if an entity has made an application under  
4 section 14 for accreditation as an accredited entity.
- 5 (2) The Digital ID Regulator must decide:  
6 (a) to accredit the entity; or  
7 (b) to refuse to accredit the entity.
- 8 (3) The Digital ID Regulator must not accredit an entity:  
9 (a) as an accredited attribute service provider unless the entity is  
10 an attribute service provider; or  
11 (b) as an accredited identity exchange provider unless the entity  
12 is an identity exchange provider; or  
13 (c) as an accredited identity service provider unless the entity is  
14 an identity service provider; or  
15 (d) if Accreditation Rules made for the purposes of paragraph  
16 14(1)(d) prescribe services—as an entity that provides  
17 services of the kind prescribed unless the entity provides  
18 services of that kind.
- 19 (4) The Digital ID Regulator must not accredit an entity if:  
20 (a) a direction under subsection 16(1) (about security) is in force  
21 in relation to the entity; or  
22 (b) if the Digital ID Regulator makes a requirement under  
23 paragraph 126(1)(a) in relation to the entity—the Digital ID  
24 Regulator is not satisfied that the entity has been assessed as  
25 being able to comply with this Act; or  
26 (c) Accreditation Rules made for the purposes of section 27  
27 require specified criteria to be met and the entity does not  
28 meet the criteria; or  
29 (d) Accreditation Rules made for the purposes of section 27  
30 require the Digital ID Regulator be satisfied of specified  
31 matters and the Digital ID Regulator is not satisfied of those  
32 matters.

# EXPOSURE DRAFT

Accreditation **Chapter 2**

Accreditation **Part 2**

Accreditation **Division 2**

## Section 15

---

- 1 (5) In deciding whether to accredit the entity, the Digital ID Regulator:  
2 (a) must have regard to the matters (if any) prescribed by the  
3 Accreditation Rules; and  
4 (b) may consult:  
5 (i) the Information Commissioner; or  
6 (ii) the Australian Securities and Investments Commission;  
7 or  
8 (iii) the Australian Prudential Regulation Authority; or  
9 (iv) the Australian Financial Complaints Authority; or  
10 (v) the part of the Australian Signals Directorate known as  
11 the Australian Cyber Security Centre; or  
12 (vi) any other body the Digital ID Regulator considers  
13 appropriate; and  
14 (c) may have regard to the following:  
15 (i) matters raised in consultations (if any) under  
16 paragraph (b);  
17 (ii) matters relating to security (within the meaning of the  
18 *Australian Security Intelligence Organisation Act*  
19 *1979*);  
20 (iii) whether the entity is a fit and proper person;  
21 (iv) any other matters the Digital ID Regulator considers  
22 relevant.
- 23 Note: In having regard to whether an entity is a fit and proper person for the  
24 purposes of subparagraph (c)(iii), the Digital ID Regulator must have  
25 regard to any matters specified in the Digital ID Rules and may have  
26 regard to any other matters considered relevant (see section 12).
- 27 (6) The Digital ID Regulator must:  
28 (a) give written notice of a decision to accredit, or to refuse to  
29 accredit, the entity; and  
30 (b) if the decision is to refuse to accredit the entity—give reasons  
31 for the decision to the entity.
- 32 (7) If the Digital ID Regulator decides to accredit the entity, the notice  
33 must also set out the following:  
34 (a) the kind of accredited entity that the entity is accredited as;  
35 (b) the day the accreditation comes into force;
-

# EXPOSURE DRAFT

Chapter 2 Accreditation

Part 2 Accreditation

Division 2 Accreditation

## Section 16

---

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

### 3 **16 Minister's directions regarding accreditation**

- 4 (1) The Minister may, in writing, direct the Digital ID Regulator to  
5 refuse to accredit an entity if, for reasons of security (within the  
6 meaning of the *Australian Security Intelligence Organisation Act*  
7 *1979*), including on the basis of an adverse or qualified security  
8 assessment in respect of a person, the Minister considers it  
9 appropriate to do so.
- 10 (2) The Minister may, in writing, direct the Digital ID Regulator to  
11 suspend the accreditation of an accredited entity (either indefinitely  
12 or for a specified period) if, for reasons of security (within the  
13 meaning of the *Australian Security Intelligence Organisation Act*  
14 *1979*), including on the basis of an adverse or qualified security  
15 assessment in respect of a person, the Minister considers it  
16 appropriate to do so.
- 17 (3) If the Minister gives a direction under subsection (1) or (2), the  
18 Digital ID Regulator must comply with the direction.
- 19 (4) The direction remains in force until revoked by the Minister. The  
20 Minister must notify the Digital ID Regulator and the entity if the  
21 Minister revokes the direction.
- 22 Note: The entity cannot be accredited again while the direction remains in  
23 force (see paragraph 15(4)(a)).
- 24 (5) A direction given under subsection (1) or (2) is not a legislative  
25 instrument.

### 26 **17 Accreditation is subject to conditions**

- 27 (1) The accreditation of an entity as an accredited entity is subject to  
28 the following conditions (the *accreditation conditions*):  
29 (a) the conditions set out in subsection 18(1);



- 1 (b) the conditions (if any) imposed by the Digital ID Regulator  
2 under subsection 18(2), including as varied under  
3 subsection 20(1);  
4 (c) the conditions (if any) determined by the Accreditation Rules  
5 under subsection 18(6).

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

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

## 11 **18 Conditions on accreditation**

### 12 *Conditions imposed by the Act*

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

### 15 *Conditions imposed by the Digital ID Regulator*

- 16 (2) The Digital ID Regulator may impose conditions on the  
17 accreditation of an entity, either at the time of accreditation or at a  
18 later time, if the Digital ID Regulator considers that doing so is  
19 appropriate in the circumstances.
- 20 (3) Conditions may be imposed under subsection (2) on application by  
21 the entity or on the Digital ID Regulator's own initiative.
- 22 (4) Without limiting subsection (2), a condition may be imposed for  
23 reasons of security (within the meaning of the *Australian Security*  
24 *Intelligence Organisation Act 1979*), including on the basis of an  
25 adverse or qualified security assessment in respect of a person.
- 26 (5) Without limiting subsection (2), the Digital ID Regulator may  
27 impose conditions relating to the following:  
28 (a) any limitations, exclusions or restrictions in relation to the  
29 accredited services of the entity;  
30 (b) the circumstances or manner in which the accredited services  
31 of the entity must be provided;

# EXPOSURE DRAFT

Chapter 2 Accreditation

Part 2 Accreditation

Division 2 Accreditation

## Section 19

---

- 1 (c) the kinds of restricted attributes of individuals (if any) that  
2 the entity is authorised to collect or disclose and the  
3 circumstances in which such attributes may be collected or  
4 disclosed;
- 5 (d) the kinds of biometric information (if any) of an individual  
6 the entity is authorised to collect, use or disclose and the  
7 circumstances in which such information may be collected,  
8 used or disclosed;
- 9 (e) the entity's information technology systems through which  
10 the entity's accredited services are provided, including  
11 restrictions on changes to such systems;
- 12 (f) actions that the entity must take before the entity's  
13 accreditation is suspended or revoked.

### 14 *Conditions imposed by the Accreditation Rules*

- 15 (6) The Accreditation Rules may determine that the accreditation of  
16 each accredited entity, or each accredited entity included in a  
17 specified class, is subject to specified conditions.
- 18 (7) Without limiting subsection (6), the Accreditation Rules may  
19 impose conditions relating to the matters in subsection (5).

### 20 **19 Requirements before Accreditation Rules impose conditions** 21 **relating to restricted attributes or biometric information** 22 **of individuals**

- 23 (1) Subsection (2) applies if the Minister proposes to make  
24 Accreditation Rules for the purposes of subsection 18(6) providing  
25 that accredited entities, or specified kinds of accredited entities, are  
26 authorised to:
- 27 (a) collect or disclose restricted attributes of individuals; or  
28 (b) collect, use or disclose biometric information of individuals.

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

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

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

## 10 **20 Variation and revocation of conditions on accreditation**

- 11 (1) The Digital ID Regulator may vary or revoke a condition imposed  
12 on an entity's accreditation under subsection 18(2):
- 13 (a) at any time, on the Digital ID Regulator's own initiative; or  
14 (b) on application by the entity under section 21;  
15 if the Digital ID Regulator considers it is appropriate to do so.
- 16 (2) Without limiting subsection (1), the Digital ID Regulator may have  
17 regard to the following matters when considering whether it is  
18 appropriate to vary or revoke a condition:
- 19 (a) matters relating to the security, reliability and stability of the  
20 Australian Government Digital ID System;
- 21 (b) matters relating to security (within the meaning of the  
22 *Australian Security Intelligence Organisation Act 1979*).

## 23 **21 Applying for variation or revocation of conditions on** 24 **accreditation**

- 25 (1) An accredited entity may apply for a condition on the entity's  
26 accreditation to be varied or revoked.
- 27 Note: See Part 5 of Chapter 8 for matters relating to applications.
- 28 (2) If, after receiving an application under subsection (1), the Digital  
29 ID Regulator refuses to vary or revoke a condition, the Digital ID  
30 Regulator must give to the entity written notice of the refusal,  
31 including reasons for the refusal.

# EXPOSURE DRAFT

Chapter 2 Accreditation

Part 2 Accreditation

Division 2 Accreditation

## Section 22

---

### 22 Notice before changes to conditions on accreditation

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30

- (1) The Digital ID Regulator must not, on the Digital ID Regulator's own initiative:
  - (a) impose a condition under subsection 18(2) on an entity's accreditation after the entity has been accredited; or
  - (b) vary or revoke a condition under subsection 20(1);unless the Digital ID Regulator has given the entity a written notice in accordance with subsection (2).
- (2) The notice must:
  - (a) state the proposed condition, variation or revocation; and
  - (b) request the entity to give the Digital ID Regulator, within the period specified in the notice, a written statement relating to the proposed condition, variation or revocation.
- (3) The Digital ID Regulator must consider any written statement given within the period specified in the notice before making a decision to:
  - (a) impose a condition under subsection 18(2) on an entity's accreditation; or
  - (b) vary or revoke a condition under subsection 20(1) on an entity's accreditation.
- (4) This section does not apply if the Digital ID Regulator reasonably believes that the need to impose, vary or revoke the condition is serious and urgent.
- (5) If this section does not apply to an entity because of subsection (4), the Digital ID Regulator must give a written statement of reasons to the entity as to why the Digital ID Regulator reasonably believes that the need to impose, vary or revoke the condition is serious and urgent.
- (6) The statement of reasons must be given within 7 days after the condition is imposed, varied or revoked.

# EXPOSURE DRAFT

Accreditation **Chapter 2**

Accreditation **Part 2**

Accreditation **Division 2**

Section 23

---

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

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12

- (1) Subject to subsection (2), the Digital ID Regulator must give an entity written notice of a decision to impose, vary or revoke a condition on an entity's accreditation.
- (2) The Digital ID Regulator is not required to give an entity notice of the decision if notice of the condition was given in a notice under subsection 15(7).
- (3) The notice must:
  - (a) state the condition or the variation, or state that the condition is revoked; and
  - (b) state the day on which the condition, variation or revocation takes effect.

# EXPOSURE DRAFT

Chapter 2 Accreditation

Part 2 Accreditation

Division 3 Varying, suspending and revoking accreditation

Section 24

---

1 **Division 3—Varying, suspending and revoking**  
2 **accreditation**

3 **24 Varying accreditation**

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

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

9 **25 Suspension of accreditation**

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

12 (1) The Digital ID Regulator must, in writing, suspend the  
13 accreditation of an accredited entity if a direction under subsection  
14 16(2) is in force in relation to the entity.

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

17 (2) The Digital ID Regulator may, in writing, suspend the  
18 accreditation of an accredited entity if:  
19 (a) the Digital ID Regulator reasonably believes that the  
20 accredited entity has contravened or is contravening this Act;  
21 or  
22 (b) the Digital ID Regulator reasonably believes that there has  
23 been a cyber security incident involving the entity; or  
24 (c) the Digital ID Regulator reasonably believes that a cyber  
25 security incident involving the entity is imminent; or  
26 (d) the Digital ID Regulator reasonably believes that, for reasons  
27 of security (within the meaning of the *Australian Security*  
28 *Intelligence Organisation Act 1979*), including on the basis  
29 of an adverse or qualified security assessment in respect of a  
30 person, it is appropriate to do so; or

# EXPOSURE DRAFT

Accreditation **Chapter 2**

Accreditation **Part 2**

Varying, suspending and revoking accreditation **Division 3**

## Section 25

---

- 1 (e) if the entity is a body corporate—the entity becomes a  
2 Chapter 5 body corporate (within the meaning of the  
3 *Corporations Act 2001*); or  
4 (f) the Digital ID Regulator is satisfied that it is not appropriate  
5 for the entity to be an accredited entity; or  
6 (g) circumstances specified in the Accreditation Rules apply in  
7 relation to the entity.

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

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

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

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

20 *Digital ID Regulator may suspend accreditation on application*

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

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

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

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

- 29 (7) The show cause notice must:

- 30 (a) state the grounds on which the Digital ID Regulator proposes  
31 to suspend the entity's accreditation; and  
32 (b) invite the entity to give the Digital ID Regulator, within 28  
33 days after the day the notice is given, a written statement
-

# EXPOSURE DRAFT

## Chapter 2 Accreditation

### Part 2 Accreditation

#### Division 3 Varying, suspending and revoking accreditation

##### Section 25

---

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

3 *Exception—cyber security incident*

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

6 *Notice of suspension*

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

- 10 (a) that the entity's accreditation is suspended;  
11 (b) if the entity is accredited as more than one kind of accredited  
12 entity—the accreditation that is suspended;  
13 (c) the reasons for the suspension;  
14 (d) the day the suspension is to start;  
15 (e) if the accreditation is suspended for a period—the period of  
16 the suspension;  
17 (f) if the accreditation is suspended until a specified event  
18 occurs or action is taken—the event or action;  
19 (g) if the accreditation is suspended indefinitely—that fact.

20 *Effect of suspension*

- 21 (10) If an entity's accreditation is suspended under this section:  
22 (a) the entity is taken not to be accredited while the suspension is  
23 in force; and  
24 (b) if the entity holds an approval to participate in the Australian  
25 Government Digital ID System—the entity is taken not to  
26 hold the approval while the entity's accreditation is  
27 suspended.



# EXPOSURE DRAFT

Accreditation **Chapter 2**

Accreditation **Part 2**

Varying, suspending and revoking accreditation **Division 3**

Section 26

---

1

## *Revocation of suspension*

2

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

3

4

5

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

6

7

8

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

9

10

11

12

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

13

14

## **26 Revocation of accreditation**

15

### *Revocation on Digital ID Regulator's own initiative*

16

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

17

18

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

19

20

21

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

22

23

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

24

25

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

26

27

28

29

30

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

31

32

# EXPOSURE DRAFT

## Chapter 2 Accreditation

### Part 2 Accreditation

#### Division 3 Varying, suspending and revoking accreditation

#### Section 26

---

- 1 (f) the Digital ID Regulator is satisfied that it is not appropriate  
2 for the entity to be an accredited entity; or  
3 (g) circumstances specified in the Accreditation Rules apply in  
4 relation to the entity.

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

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

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

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

#### 17 *Revocation on application*

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

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

#### 21 *Date of effect*

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

#### 24 *Approval must also be revoked*

- 25 (6) If:  
26 (a) an entity's accreditation is revoked under subsection (1) or  
27 (4); and  
28 (b) the entity holds an approval to participate in the Australian  
29 Government Digital ID System;  
30 the Digital ID Regulator must at the same time revoke the entity's  
31 approval to participate.

# EXPOSURE DRAFT

Accreditation **Chapter 2**

Accreditation **Part 2**

Varying, suspending and revoking accreditation **Division 3**

## Section 26

---

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

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

6                    (8) The show cause notice must:

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

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

13                    *Exception—cyber security incident*

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

16                    *Notice of revocation*

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

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

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

23                        (c) the reasons for the revocation;

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

25                    *Accreditation can be revoked even while suspended*

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

# EXPOSURE DRAFT

Chapter 2 Accreditation

Part 2 Accreditation

Division 4 Accreditation Rules

Section 27

---

1 **Division 4—Accreditation Rules**

2 **27 Accreditation Rules**

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

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

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

10 (i) privacy;

11 (ii) security;

12 (iii) fraud control;

13 (iv) incident management and reporting;

14 (v) disaster recovery;

15 (vi) user experience and inclusion;

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

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

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

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

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

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

# EXPOSURE DRAFT

Accreditation **Chapter 2**  
Accreditation **Part 2**  
Accreditation Rules **Division 4**

## Section 27

---

- 1 (h) matters relating to representatives or nominees of individuals  
2 in relation to the creation, maintenance or deactivation of  
3 digital IDs of individuals;  
4 (i) requirements or restrictions relating to the generation of  
5 digital IDs for children.

6 Note: In relation to subparagraph (2)(a)(iv), the Digital ID Rules may also  
7 provide for such arrangements in relation to incidents that occur  
8 within the Australian Government Digital ID System (see subsection  
9 74(1)).

# EXPOSURE DRAFT

Chapter 2 Accreditation

Part 2 Accreditation

Division 5 Other matters relating to accredited entities

Section 28

---

1 **Division 5—Other matters relating to accredited entities**

2 **28 Digital IDs must be deactivated on request**

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

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

8 **29 Accredited services must be accessible and inclusive**

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

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

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

16 (b) requirements relating to useability testing;

17 (c) requirements relating to device or browser access.

1 **Chapter 3—Privacy**

2 **Part 1—Introduction**  
3

4 **30 Simplified outline of this Chapter**

5 **31 Chapter applies to accredited entities only to the extent the entity**  
6 **is providing accredited services etc.**

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

- 9 (a) providing its accredited services; or  
10 (b) doing things that are incidental or ancillary to the provision  
11 of those services.

12 **32 APP-equivalent agreements**

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

# EXPOSURE DRAFT

Chapter 3 Privacy

Part 2 Privacy

Division 1 Interaction with the Privacy Act 1988

Section 33

---

1 **Part 2—Privacy**

2 **Division 1—Interaction with the Privacy Act 1988**

3 **33 Extended meaning of *personal information* in relation to**  
4 **accredited entities**

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

10 Note 1: This section has the effect of extending the meaning of personal  
11 information in the *Privacy Act 1988* as it applies to accredited entities  
12 to mirror the meaning of that term as it is used in this Act (see section  
13 9).

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

20 **34 Privacy obligations for non-APP entities**

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

23 Note: The obligations of accredited entities that are APP entities in relation  
24 to the handling of personal information are set out in the *Privacy Act*  
25 *1988*.

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

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

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



- 1 (i) protection of personal information comparable to that  
2 provided by the Australian Privacy Principles;  
3 (ii) monitoring of compliance with the law;  
4 (iii) a means for an individual to seek recourse if the  
5 individual's personal information is dealt with in a way  
6 contrary to the law; or  
7 (c) all of the following apply:  
8 (i) neither paragraph (a) nor (b) apply to the acts or  
9 practices of the entity;  
10 (ii) the entity has an APP-equivalent agreement with the  
11 Commonwealth;  
12 (iii) the agreement includes a term that prohibits the entity  
13 from collecting, holding, using or disclosing personal  
14 information in any way that would, if the entity were an  
15 organisation within the meaning of the *Privacy Act*  
16 *1988*, breach an Australian Privacy Principle.

## 17 **35 Contraventions of privacy obligations in APP-equivalent** 18 **agreements**

- 19 (1) This section applies to an entity if the entity has an APP-equivalent  
20 agreement with the Commonwealth.
- 21 (2) An act or practice of the entity that contravenes a term of the  
22 agreement in relation to an individual and collecting, holding,  
23 using or disclosing their personal information is taken to be:  
24 (a) an interference with the privacy of the individual for the  
25 purposes of the *Privacy Act 1988*; and  
26 (b) covered by sections 13 and 13G of that Act.
- 27 Note: An act or practice that is, or may be, an interference with privacy may  
28 be the subject of a complaint under section 36 of the *Privacy Act*  
29 *1988*.
- 30 (3) The entity is taken, for the purposes of Part V of the *Privacy Act*  
31 *1988* and any other provision of that Act that relates to that Part, to  
32 be an organisation (within the meaning of that Act) if:

# EXPOSURE DRAFT

## Chapter 3 Privacy

### Part 2 Privacy

#### Division 1 Interaction with the Privacy Act 1988

#### Section 36

---

- 1 (a) an act or practice of the entity has contravened, or may have  
2 contravened, the term of the agreement in relation to an  
3 individual; and  
4 (b) the act or practice is the subject of a complaint to, or an  
5 investigation by, the Information Commissioner under Part V  
6 of the *Privacy Act 1988*.
- 7 (4) Sections 80V and 80W of the *Privacy Act 1988* apply in relation to  
8 the term of the agreement as if the term were a provision of that  
9 Act.

#### 10 **36 Contraventions of Division 2 are interferences with privacy**

- 11 (1) An act or practice of an accredited entity that contravenes a  
12 provision of Division 2 of this Part in relation to personal  
13 information about an individual is taken to be:  
14 (a) an interference with the privacy of the individual for the  
15 purposes of the *Privacy Act 1988*; and  
16 (b) covered by sections 13 and 13G of that Act.
- 17 Note: An act or practice that is, or may be, an interference with privacy may  
18 be the subject of a complaint under section 36 of the *Privacy Act*  
19 *1988*.
- 20 (2) The respondent to a complaint under the *Privacy Act 1988* about  
21 the act or practice, other than an act or practice of an agency or  
22 organisation, is the entity that engaged in the act or practice.
- 23 (3) The entity is taken, for the purposes of Part V of the *Privacy Act*  
24 *1988* and any other provision of that Act that relates to that Part, to  
25 be an organisation if:  
26 (a) the act or practice of the entity that contravenes a provision  
27 of Division 2 of this Part is the subject of a complaint to, or  
28 an investigation by, the Information Commissioner under  
29 Part V of the *Privacy Act 1988*; and  
30 (b) the entity is not an agency or organisation.
- 31 (4) In this section:  
32 **agency** has the same meaning as in the *Privacy Act 1988*.

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

2                    **37 Notification of eligible data breaches—accredited entities that are**  
3                    **APP entities**

- 4                    (1) This section applies to an accredited entity if the entity:
- 5                    (a) is an APP entity; and
  - 6                    (b) is aware that there are reasonable grounds to believe that  
7                    there has been an eligible data breach (within the meaning of  
8                    the *Privacy Act 1988*) of the entity relating to the entity’s  
9                    accredited services; and
  - 10                    (c) is required under section 26WK of the *Privacy Act 1988* to  
11                    give the Information Commissioner a statement that complies  
12                    with subsection 26WK(3) of that Act.
- 13                    (2) The entity must also give a copy of the statement to the Digital ID  
14                    Regulator at the same time as the statement is given to the  
15                    Information Commissioner.

16                    **38 Notification of eligible data breaches—accredited entities that are**  
17                    **not APP entities**

- 18                    (1) This section applies to an accredited entity that is not an APP  
19                    entity.
- 20                    (2) Despite subsection (1), this section does not apply to an accredited  
21                    entity if:
- 22                    (a) the entity is a department or authority of a State or Territory;  
23                    and
  - 24                    (b) a law of the State or Territory provides for a scheme for the  
25                    notification of data breaches that:
    - 26                    (i) covers the entity; and
    - 27                    (ii) is comparable to the scheme provided for in Part IIIC of  
28                    the *Privacy Act 1988*.

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

# EXPOSURE DRAFT

## Chapter 3 Privacy

### Part 2 Privacy

#### Division 1 Interaction with the Privacy Act 1988

##### Section 39

---

- 1 (3) Part IIIC of the *Privacy Act 1988*, and any other provision of that  
2 Act that relates to that Part, apply in relation to the accredited  
3 entity as if the entity were an APP entity.
- 4 (4) If:
- 5 (a) the accredited entity is aware that there are reasonable  
6 grounds to believe that there has been an eligible data breach  
7 (within the meaning of the *Privacy Act 1988*) of the entity  
8 relating to the entity's accredited services; and
- 9 (b) because of the operation of subsection (3), the entity is  
10 required under section 26WK of that Act to give the  
11 Information Commissioner a statement that complies with  
12 subsection 26WK(3) of that Act;
- 13 the entity must also give a copy of the statement to the Digital ID  
14 Regulator at the same time as the statement is given to the  
15 Information Commissioner.

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

- 16  
17
- 18 (1) This section applies to an accredited entity if:
- 19 (a) the entity is not an APP entity; and
- 20 (b) the entity is a department or authority of a State or Territory;
- 21 and
- 22 (c) the entity is required under a law of the State or Territory to  
23 give a statement (however described) that corresponds to  
24 section 26WK of the *Privacy Act 1988* to another entity (the  
25 ***notified entity***); and
- 26 (d) the statement relates to the accredited services of the entity.
- 27 (2) The entity must also give a copy of the statement to the Digital ID  
28 Regulator and the Information Commissioner at the same time as  
29 the statement is given to the notified entity.

#### **40 Additional function of the Information Commissioner**

30  
31 In addition to the Information Commissioner's functions under the  
32 *Privacy Act 1988*, the Information Commissioner has the function

# EXPOSURE DRAFT

Privacy **Chapter 3**

Privacy **Part 2**

Interaction with the Privacy Act 1988 **Division 1**

Section 40

---

1  
2

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

EXPOSURE DRAFT

# EXPOSURE DRAFT

Chapter 3 Privacy

Part 2 Privacy

Division 2 Additional privacy safeguards

Section 41

---

1 **Division 2—Additional privacy safeguards**

2 **41 Collection etc. of certain attributes of individuals is prohibited**

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

- 5 (a) information or an opinion about an individual’s racial or  
6 ethnic origin;
- 7 (b) information or an opinion about an individual’s political  
8 opinions;
- 9 (c) information or an opinion about an individual’s membership  
10 of a political association;
- 11 (d) information or an opinion about an individual’s religious  
12 beliefs or affiliations;
- 13 (e) information or an opinion about an individual’s philosophical  
14 beliefs;
- 15 (f) information or an opinion about an individual’s sexual  
16 orientation or practices.

17 Civil penalty: 300 penalty units.

18 **42 Individuals must expressly consent to disclosure of certain**  
19 **attributes of individuals to relying parties**

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

- 25 (a) the individual’s name;
- 26 (b) the individual’s address;
- 27 (c) the individual’s date of birth;
- 28 (d) the individual’s phone number;
- 29 (e) the individual’s email address;
- 30 (f) an attribute of a kind prescribed by the Accreditation Rules.

1 Civil penalty: 300 penalty units.

## 2 **43 Disclosure of restricted attributes of individuals**

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

8 Civil penalty: 300 penalty units.

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

14 Civil penalty: 300 penalty units.

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

20 Civil penalty: 300 penalty units.

## 21 **44 Restricting the disclosure of unique identifiers**

22 (1) This section applies if:

- 23 (a) an accredited entity (the *assigning entity*) assigns a unique  
24 identifier to an individual within a digital ID system; and  
25 (b) the assigning entity discloses the unique identifier to another  
26 accredited entity or to a relying party.

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

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

# EXPOSURE DRAFT

## Chapter 3 Privacy

### Part 2 Privacy

#### Division 2 Additional privacy safeguards

#### Section 44

---

- 1 (b) if the unique identifier was disclosed to a relying party—the  
2 relying party.
- 3 Civil penalty: 300 penalty units.
- 4 (3) The accredited entity or relying party to whom the unique identifier  
5 is disclosed must not disclose the unique identifier to any other  
6 entity.
- 7 Civil penalty: 300 penalty units.
- 8 (4) Subsections (2) and (3) do not apply if the disclosure of the unique  
9 identifier is for one or more of the following purposes:
- 10 (a) detecting, reporting or investigating a contravention, or an  
11 alleged contravention, of a provision of this Act;
- 12 (b) conducting proceedings in relation to a contravention, or an  
13 alleged contravention, of a civil penalty provision of this Act;
- 14 (c) detecting, reporting or investigating either of the following  
15 within a digital ID system:
- 16 (i) a digital ID fraud incident;
- 17 (ii) a cyber security incident;
- 18 (d) conducting an assessment of the matter referred to in  
19 paragraph 33C(1)(g) of the *Privacy Act 1988* (about  
20 assessments by the Information Commissioner in relation to  
21 the handling and maintenance of personal information in  
22 accordance with certain aspects of this Act);
- 23 (e) detecting, reporting, investigating or prosecuting an offence  
24 against a law of the Commonwealth, a State or a Territory.
- 25 Note: A person who wishes to rely on this subsection bears an evidential  
26 burden in relation to the matter mentioned in this subsection (see  
27 section 96 of the Regulatory Powers Act).
- 28 (5) Subsections (2) and (3) also do not apply if the unique identifier is  
29 disclosed to another entity if the other entity is facilitating access to  
30 the entity for whom the unique identifier was created.
- 31 Note: A person who wishes to rely on this subsection bears an evidential  
32 burden in relation to the matter mentioned in this subsection (see  
33 section 96 of the Regulatory Powers Act).



1     **45 Restrictions on collecting, using and disclosing biometric**  
2             **information**

- 3             (1) An accredited entity may collect, use or disclose biometric  
4             information of an individual only if:  
5                 (a) the collection, use or disclosure is authorised under section  
6                 46 or 47; and  
7                 (b) unless the collection, use or disclosure is authorised under  
8                 paragraph 46(3)(a) or subsection 46(5), (6) or (8)—the  
9                 individual to whom the information relates has expressly  
10                consented to the collection, use or disclosure of the biometric  
11                information.

12             Civil penalty:             300 penalty units.

- 13             (2) To avoid doubt, and without limiting subsection (1), an accredited  
14             entity must not:  
15                 (a) collect, use or disclose biometric information of an individual  
16                 for the purpose of one-to-many matching of the individual; or  
17                 (b) collect, use or disclose biometric information of an individual  
18                 to determine whether the individual has multiple digital IDs.
- 19             (3) ***One-to-many matching*** means the process of comparing a kind of  
20             biometric information of an individual against that kind of  
21             biometric information of individuals generally to identify the  
22             particular individual.

23     **46 Authorised collection, use and disclosure of biometric**  
24             **information of individuals—general rules**

- 25             (1) An accredited entity is authorised to collect, use or disclose  
26             biometric information of an individual if:  
27                 (a) the entity is an accredited identity service provider; and  
28                 (b) the entity's conditions on accreditation authorise the  
29                 collection, use or disclosure of the biometric information;  
30                 and

# EXPOSURE DRAFT

## Chapter 3 Privacy

### Part 2 Privacy

#### Division 2 Additional privacy safeguards

#### Section 46

---

- 1 (c) the biometric information of the individual is collected, used  
2 or disclosed for the purposes of the accredited entity doing  
3 either or both of the following:  
4 (i) verifying the identity of the individual;  
5 (ii) authenticating the individual to their digital ID.
- 6 (2) An accredited entity is authorised to collect, use or disclose  
7 biometric information of an individual if:  
8 (a) the biometric information is contained in a verifiable  
9 credential that is in control of the individual; and  
10 (b) the collection, use or disclosure complies with any  
11 requirements prescribed by the Accreditation Rules.
- 12 (3) An accredited entity is authorised to disclose biometric information  
13 of an individual to a law enforcement agency (within the meaning  
14 of the *Australian Crime Commission Act 2002*) only if:  
15 (a) the information is disclosed under a warrant issued by a  
16 magistrate, judge or member of a tribunal; or  
17 (b) the information is disclosed with the consent of the  
18 individual to whom the biometric information relates, or  
19 purports to relate, and the disclosure is for the purpose of:  
20 (i) verifying the identity of the individual; or  
21 (ii) investigating or prosecuting an offence against a law of  
22 the Commonwealth, a State or a Territory.
- 23 (4) Subsection (3) applies despite any law of the Commonwealth, a  
24 State or a Territory (whether enacted or made before or after this  
25 subsection) or a warrant, authorisation or order issued under such a  
26 law.
- 27 (5) An accredited entity is authorised to disclose biometric information  
28 of an individual if the disclosure is to the individual to whom the  
29 biometric information relates.
- 30 (6) An accredited entity is authorised to retain, use or disclose  
31 biometric information of an individual if:  
32 (a) the entity is an accredited identity service provider; and

# EXPOSURE DRAFT

- 1 (b) the entity collected the information in accordance with  
2 subsection (1); and
- 3 (c) the information is retained, used or disclosed for the purposes  
4 of undertaking testing in relation to the information; and
- 5 (d) the entity complies with any requirements prescribed by the  
6 Accreditation Rules.
- 7 (7) Without limiting paragraph (6)(d), Accreditation Rules made for  
8 the purposes of that paragraph may prescribe requirements in  
9 relation to the following matters:
- 10 (a) the purposes for which testing may be undertaken;
- 11 (b) the kinds of testing that may be undertaken using biometric  
12 information;
- 13 (c) the circumstances in which testing of the biometric  
14 information may be undertaken;
- 15 (d) the manner in which the biometric information that has been  
16 retained for testing must be destroyed;
- 17 (e) the preparation, content, approval and implementation of  
18 ethics plans relating to the testing of the biometric  
19 information;
- 20 (f) obtaining express consent of individuals to whom the  
21 biometric information relates;
- 22 (g) reporting of testing results to the Digital ID Regulator.
- 23 (8) An accredited entity is authorised to retain, use or disclose  
24 biometric information of an individual if:
- 25 (a) the entity is an accredited identity service provider; and
- 26 (b) the entity collected the information in accordance with  
27 subsection (1); and
- 28 (c) the information is retained, used or disclosed for the purposes  
29 of preventing or investigating a digital ID fraud incident; and
- 30 (d) the entity complies with any requirements prescribed by the  
31 Accreditation Rules.
- 32 (9) Without limiting paragraph (8)(d), Accreditation Rules made for  
33 the purposes of that paragraph may prescribe requirements in  
34 relation to the following matters:

# EXPOSURE DRAFT

## Chapter 3 Privacy

### Part 2 Privacy

#### Division 2 Additional privacy safeguards

#### Section 47

---

- 1 (a) the manner in which biometric information that has been  
2 retained for preventing or investigating digital ID fraud  
3 incidents must be destroyed;  
4 (b) the reporting of fraud prevention or investigation activities to  
5 the Digital ID Regulator.

6 **47 Accredited identity service providers may collect etc. biometric**  
7 **information for purposes of government identity**  
8 **documents**

- 9 (1) This section applies if:  
10 (a) an accredited entity collects biometric information of an  
11 individual under subparagraph 46(1)(c)(i) for the purpose of  
12 verifying the identity of the individual; and  
13 (b) the accredited entity has verified that the biometric  
14 information is legitimate.
- 15 Note: Because this Chapter applies to an entity only to the extent that the  
16 entity is providing accredited services or doing things that are  
17 incidental or ancillary to the provision of those services (see  
18 section 31), this section does not affect information collected,  
19 retained, etc. by the entity in any other capacity.
- 20 (2) If the entity is covered by subsection (3), the entity may collect,  
21 use, disclose or retain the biometric information for the purposes of  
22 issuing a document or other credential that:  
23 (a) contains personal information about the individual; and  
24 (b) the individual has consented to the issue of; and  
25 (c) can be used to assist the individual to prove the individual's  
26 age or identity or a permission or authorisation that the  
27 individual holds; and  
28 (d) is issued by or on behalf of the entity.
- 29 (3) The entities covered by this subsection are as follows:  
30 (a) a body corporate incorporated by or under a law of the  
31 Commonwealth or a State or Territory;  
32 (b) a Commonwealth entity, or a Commonwealth company,  
33 within the meaning of the *Public Governance, Performance*  
34 *and Accountability Act 2013*; or

# EXPOSURE DRAFT

## Section 48

---

- 1 (c) a person or body that is an agency within the meaning of the  
2 *Freedom of Information Act 1982*;
- 3 (d) a body specified, or the person holding an office specified, in  
4 Part I of Schedule 2 to the *Freedom of Information Act 1982*;
- 5 (e) a department or authority of a State;
- 6 (f) a department or authority of a Territory.
- 7 (4) Subsection (2) applies despite anything else in this Division.
- 8 (5) If:
- 9 (a) the entity (the *first entity*) is not covered by subsection (3);  
10 and
- 11 (b) the first entity has a written agreement with another entity  
12 (the *government entity*) that is covered by that subsection;  
13 and
- 14 (c) the agreement provides for the first entity to disclose the  
15 biometric information of the individual to the government  
16 entity for the purposes of issuing a document or other  
17 credential that:
- 18 (i) contains personal information about the individual; and  
19 (ii) the individual has consented to the issue of; and  
20 (iii) can be used to assist the individual to prove the  
21 individual's age or identity or a permission or  
22 authorisation that the individual holds; and  
23 (iv) is issued by or on behalf of the entity;
- 24 the entity may disclose the biometric information in accordance  
25 with the agreement if the disclosure occurs within 14 days after the  
26 biometric information is collected.

### 48 Destruction of biometric information of individuals

- 28 (1) Subject to subsections (3) and (4), if an accredited identity service  
29 provider collects biometric information of an individual for the  
30 purposes of verifying an individual's identity, the provider must  
31 destroy the information immediately after the verification is  
32 complete.
- 33 Civil penalty: 300 penalty units.

# EXPOSURE DRAFT

## Chapter 3 Privacy

### Part 2 Privacy

#### Division 2 Additional privacy safeguards

#### Section 49

---

- 1 (2) Subject to subsections (3) and (4), if:  
2 (a) an accredited entity collects biometric information of an  
3 individual with the express consent of the individual to  
4 whom the information relates; and  
5 (b) the information is collected for the purposes of authenticating  
6 the individual to their digital ID; and  
7 (c) the individual withdraws their consent;  
8 the provider must destroy the information immediately after the  
9 consent is withdrawn.
- 10 (3) If an accredited entity retains biometric information of an  
11 individual in accordance with subsection 46(6) (about testing), the  
12 entity must destroy the information at the earlier of:  
13 (a) the completion of testing the information; and  
14 (b) 14 days after the entity collects the information.
- 15 Civil penalty: 300 penalty units.
- 16 (4) If an accredited entity retains biometric information of an  
17 individual in accordance with subsection 46(8) (about preventing  
18 investigating digital ID fraud incidents), the entity must destroy the  
19 information at the earlier of:  
20 (a) immediately after the completion of activities relating to the  
21 prevention or investigation of the digital ID fraud incident (as  
22 the case may be); and  
23 (b) 14 days after the entity collects the information.
- 24 Civil penalty: 300 penalty units.

#### 49 Other rules relating to biometric information

- 25  
26 (1) The Accreditation Rules may provide for and in relation to the  
27 collection, use, disclosure, storage or destruction of biometric  
28 information of individuals by accredited entities.
- 29 (2) Without limiting subsection (1), the Accreditation Rules may  
30 provide for requirements relating to quality, security or fraud.

## 50 Data profiling to track online behaviour is prohibited

- (1) An accredited entity must not use or disclose information if:
- (a) the information is personal information about an individual that is in the entity's possession or control; and
  - (b) the information is any of the following:
    - (i) information about the services provided by the entity that the individual has accessed, or attempted to access;
    - (ii) information relating to how or when access was obtained or attempted to be obtained by the individual;
    - (iii) information relating to the method of access or attempted access by the individual;
    - (iv) the date and time the individual's identity was verified.

Civil penalty: 300 penalty units.

- (2) Subsection (1) applies even if the individual has consented to the use or disclosure.
- (3) However, subsection (1) does not apply if the use or disclosure:
- (a) is for purposes relating to the provision the entity's accredited services (including improving the performance or useability of the entity's information technology systems through which those services are provided); or
  - (b) is for the purposes of the entity complying with this Act; or
  - (c) is required or authorised by or under a law of the Commonwealth, a State or a Territory.

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

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

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

# EXPOSURE DRAFT

## Chapter 3 Privacy

### Part 2 Privacy

#### Division 2 Additional privacy safeguards

#### Section 51

---

- 1 (a) at the time the information is used or disclosed, the  
2 accredited entity is satisfied that the enforcement body  
3 reasonably suspects that a person has committed an offence  
4 against a law of the Commonwealth, a State or a Territory, or  
5 started proceedings against a person for such an offence; or  
6 (b) at the time the information is used or disclosed, the  
7 accredited entity is satisfied that the enforcement body  
8 reasonably suspects that a person has breached a law  
9 imposing a penalty or sanction, or has started proceedings  
10 against a person in relation to the breach; or  
11 (c) the information is used or disclosed under a warrant issued  
12 by a magistrate, judge or member of a tribunal; or  
13 (d) the information is used or disclosed for the purposes of  
14 reporting a suspected or actual digital ID fraud incident or  
15 suspected or actual cyber security incident; or  
16 (e) the information is used or disclosed by the accredited entity  
17 for the purposes of complying with this Act.

18 Civil penalty: 300 penalty units.

- 19 (2) Despite section 96 of the Regulatory Powers Act, in proceedings  
20 for a civil penalty order against a person for a contravention of  
21 subsection (1), the person does not bear an evidential burden in  
22 relation to the matter in paragraphs (1)(a) to (e).
- 23 (3) This section applies despite:
- 24 (a) section 86E of the *Crimes Act 1914* (about disclosure of  
25 personal information to certain entities for integrity  
26 purposes); and  
27 (b) any other law of the Commonwealth, a State or a Territory,  
28 whether enacted or made before or after the commencement  
29 of this section.



1     **52 Personal information must not be used or disclosed for**  
2             **prohibited marketing purposes**

- 3             (1) An accredited entity must not use or disclose personal information  
4                 about an individual that is in the entity's possession or control for  
5                 any of the following purposes:  
6                     (a) offering to supply goods or services;  
7                     (b) advertising or promoting goods or services;  
8                     (c) enabling another entity to offer to supply goods or services;  
9                     (d) enabling another entity to advertise or promote goods or  
10                     services;  
11                     (e) market research.

12             Civil penalty:             300 penalty units.

- 13             (2) Subsection (1) does not apply to the disclosure of personal  
14                 information about an individual if:  
15                     (a) the information is disclosed to an individual for the purposes  
16                     of:  
17                         (i) offering to supply the entity's accredited services; or  
18                         (ii) advertising or promoting the entity's accredited  
19                         services; and  
20                     (b) the information is disclosed to the individual with the  
21                     individual's express consent.

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

25     **53 Accredited identity exchange providers must not retain certain**  
26             **attributes of individuals**

- 27             (1) This section applies if, during an authenticated session, an  
28                 accredited identity exchange provider receives any of the following  
29                 attributes of an individual:  
30                     (a) a restricted attribute of the individual;  
31                     (b) the individual's name;  
32                     (c) the individual's address;

# EXPOSURE DRAFT

Chapter 3 Privacy

Part 2 Privacy

Division 2 Additional privacy safeguards

## Section 53

---

- 1 (d) the individual's date of birth;  
2 (e) the individual's phone number;  
3 (f) the individual's email address;  
4 (g) an attribute of a kind prescribed by the Accreditation Rules.
- 5 (2) The accredited identity exchange provider must not retain the  
6 attribute of the individual after the end of the authenticated session.
- 7 Civil penalty: 300 penalty units.
- 8 (3) In this section:
- 9 *authenticated session* has the meaning given by the Accreditation  
10 Rules.

# EXPOSURE DRAFT

The Australian Government Digital ID System **Chapter 4**  
Introduction **Part 1**

Section 54

---

1 **Chapter 4—The Australian Government**  
2 **Digital ID System**

3 **Part 1—Introduction**  
4

5 **54 Simplified outline of this Chapter**

# EXPOSURE DRAFT

Chapter 4 The Australian Government Digital ID System

Part 2 The Australian Government Digital ID System

Division 1 The Australian Government Digital ID System

Section 55

---

1 **Part 2—The Australian Government Digital ID**  
2 **System**

3 **Division 1—The Australian Government Digital ID System**

4 **55 Digital ID Regulator must oversee and maintain the Australian**  
5 **Government Digital ID System**

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

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

11 **56 Circumstances in which entities may provide or receive services**  
12 **within the Australian Government Digital ID System**

13 (1) An entity mentioned in column 1 of an item in the following table  
14 may provide or receive services within the Australian Government  
15 Digital ID System if the entity satisfies the requirements set out in  
16 column 2 of that item.  
17

---

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

---

<b>Item</b>	<b>Column 1 Entity</b>	<b>Column 2 Requirements</b>
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 59 to participate in the system; and (b) the participation start day for the

---

# EXPOSURE DRAFT

The Australian Government Digital ID System **Chapter 4**

The Australian Government Digital ID System **Part 2**

The Australian Government Digital ID System **Division 1**

Section 56

---

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

---

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

---

# EXPOSURE DRAFT

**Chapter 4** The Australian Government Digital ID System

**Part 2** The Australian Government Digital ID System

**Division 1** The Australian Government Digital ID System

## Section 56

---

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

---

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

---

- 1                   (2) An entity contravenes this subsection if:
- 2                    (a) the entity provides or receives services within the Australian
- 3                    Government Digital ID System; and
- 4                    (b) the entity is not an entity mentioned in column 1 of an item
- 5                    in the table in subsection (1).
- 6                    Civil penalty:           200 penalty units.
- 7                   (3) An entity contravenes this subsection if:
- 8                    (a) the entity provides or receives services within the Australian
- 9                    Government Digital ID System; and
- 10                   (b) the entity is an entity mentioned in column 1 of an item in the
- 11                    table in subsection (1); and
- 12                    (c) the entity does not satisfy one or more requirements set out in
- 13                    column 2 of that item.
-

# EXPOSURE DRAFT

The Australian Government Digital ID System **Chapter 4**

The Australian Government Digital ID System **Part 2**

The Australian Government Digital ID System **Division 1**

Section 56

---

1

Civil penalty: 200 penalty units.

EXPOSURE DRAFT

# EXPOSURE DRAFT

**Chapter 4** The Australian Government Digital ID System

**Part 2** The Australian Government Digital ID System

**Division 2** Participating in the Australian Government Digital ID System

Section 57

---

1           **Division 2—Participating in the Australian Government**  
2                           **Digital ID System**

3           **57 Phasing-in of participation in the Australian Government Digital**  
4                           **ID System**

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

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

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

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

14                                       (b) kinds of relying parties; or

15                                       (c) kinds of accredited entities; or

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

17                          (3) The Minister:

18                                       (a) must not revoke the determination; and

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

21           **58 Applying for approval to participate in the Australian**  
22                           **Government Digital ID System**

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

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

26                                       (b) the entity is:

27   (i) an accredited entity; or

28   (ii) an entity that has applied for accreditation under section  
29   14; or

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



# EXPOSURE DRAFT

The Australian Government Digital ID System **Chapter 4**  
The Australian Government Digital ID System **Part 2**  
Participating in the Australian Government Digital ID System **Division 2**

## Section 59

---

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

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

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

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

7 (a) the entity is:

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

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

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

16 (b) the entity is covered by a determination made under section  
17 57.

## 18 **59 Approval to participate in the Australian Government Digital ID** 19 **System**

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

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

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

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

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

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

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

# EXPOSURE DRAFT

**Chapter 4** The Australian Government Digital ID System

**Part 2** The Australian Government Digital ID System

**Division 2** Participating in the Australian Government Digital ID System

## Section 59

---

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

- 4 (a) matters relating to security (within the meaning of the  
5 *Australian Security Intelligence Organisation Act 1979*);  
6 (b) whether the entity is a fit and proper person;  
7 (c) whether the entity has appropriate procedures for dealing  
8 with the identities (whether real or not, and whether assumed  
9 or not) of shielded persons.

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

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

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

20 (5) The Digital ID Regulator must:

- 21 (a) give written notice of a decision to approve, or to refuse to  
22 approve, an entity to participate in the Australian  
23 Government Digital ID System; and  
24 (b) if the decision is to refuse to approve the entity—give  
25 reasons for the decision to the entity.

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

- 28 (a) the day the approval comes into force; and  
29 (b) any conditions imposed on the approval under subsection  
30 62(2); and  
31 (c) the day on which the entity must begin to participate in the  
32 Australian Government Digital ID System.

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

# EXPOSURE DRAFT

The Australian Government Digital ID System **Chapter 4**  
The Australian Government Digital ID System **Part 2**  
Participating in the Australian Government Digital ID System **Division 2**

## Section 60

---

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

### 3 **60 Minister's directions regarding participation**

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

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

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

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

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

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

### 27 **61 Approval to participate in the Australian Government Digital ID** 28 **System is subject to conditions**

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

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

# EXPOSURE DRAFT

**Chapter 4** The Australian Government Digital ID System

**Part 2** The Australian Government Digital ID System

**Division 2** Participating in the Australian Government Digital ID System

## Section 62

---

- 1 (b) the conditions (if any) imposed by the Digital ID Regulator  
2 under subsection 62(2), including as varied under  
3 subsection 64(1);  
4 (c) the conditions (if any) determined by the Digital ID Rules for  
5 the purposes of subsection 62(6).

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

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

## 12 **62 Conditions on approval to participate in the Australian** 13 **Government Digital ID System**

### 14 *Conditions imposed by the Act*

- 15 (1) The approval of an entity to participate in the Australian  
16 Government Digital ID System is subject to the following  
17 conditions:  
18 (a) unless the entity is a relying party—the entity must be an  
19 accredited entity;  
20 (b) if the entity is an accredited entity:  
21 (i) the entity must participate in the Australian Government  
22 Digital ID System only as the kind of accredited entity it  
23 is accredited as; and  
24 (ii) the entity must provide only its accredited services in  
25 the Australian Government Digital ID System;  
26 (c) the entity must begin to participate in the Australian  
27 Government Digital ID System on the entity's participation  
28 start day;  
29 (d) the entity must comply with this Act.

### 30 *Conditions imposed by the Digital ID Regulator*

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

# EXPOSURE DRAFT

- 1 System, either at the time of approval or at a later time, if the  
2 Digital ID Regulator considers that doing so is appropriate in the  
3 circumstances.
- 4 (3) Conditions may be imposed under subsection (2) on application by  
5 the entity or on the Digital ID Regulator’s own initiative.
- 6 (4) Without limiting subsection (2), a condition may be imposed for  
7 reasons of security (within the meaning of the *Australian Security*  
8 *Intelligence Organisation Act 1979*), including on the basis of an  
9 adverse or qualified security assessment in respect of a person.
- 10 (5) Without limiting subsection (2), the Digital ID Regulator may  
11 impose conditions that relate to any of the following:
- 12 (a) the kind of accredited entity or participating relying party  
13 that the entity must directly connect to in order to participate  
14 in the Australian Government Digital ID System;
- 15 (b) the kinds of attributes of individuals that the entity is  
16 authorised to collect or disclose and the circumstances in  
17 which such attributes may be collected or disclosed;
- 18 (c) for an accredited entity—the circumstances in which the  
19 entity may or must not provide its accredited services within  
20 the Australian Government Digital ID System;
- 21 (d) for a relying party—the services the relying party is approved  
22 to provide, or to provide access to, within the Australian  
23 Government Digital ID System;
- 24 (e) for an accredited entity—the accredited services of the entity  
25 that the entity must provide within the Australian  
26 Government Digital ID System;
- 27 (f) actions that the entity must take before the entity’s approval  
28 to participate in the Australian Government Digital ID  
29 System is suspended or revoked.

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

# EXPOSURE DRAFT

**Chapter 4** The Australian Government Digital ID System

**Part 2** The Australian Government Digital ID System

**Division 2** Participating in the Australian Government Digital ID System

## Section 63

---

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

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

### 10 *Conditions imposed by the Digital ID Rules*

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

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

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

## 22 **63 Conditions relating to restricted attributes of individuals**

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

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

- 28 (a) to collect or disclose a restricted attribute of an individual  
29 within the Australian Government Digital ID System; or  
30 (b) to disclose a restricted attribute of an individual that is  
31 collected by the entity within the Australian Government  
32 Digital ID System to an entity outside the system.

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

---

# EXPOSURE DRAFT

- 1 (a) whether the entity has provided sufficient justification for the  
2 need to collect or disclose the restricted attribute;
- 3 (b) whether the entity has demonstrated that a similar outcome  
4 cannot be achieved without collecting or disclosing the  
5 restricted attribute;
- 6 (c) if the collection or disclosure of the restricted attribute is  
7 regulated by other legislative or regulatory requirements—  
8 whether the entity has demonstrated that it can comply with  
9 those requirements;
- 10 (d) the potential harm that could result if restricted attributes of  
11 that kind were disclosed to an entity that was not authorised  
12 to collect them;
- 13 (e) community expectations as to whether restricted attributes of  
14 that kind should be handled more securely than other kinds of  
15 attributes;
- 16 (f) any of the following information provided by the entity  
17 seeking authorisation to collect or disclose the restricted  
18 attribute:
- 19 (i) the entity’s risk assessment plan as it relates to the  
20 restricted attribute;
- 21 (ii) the entity’s privacy impact assessment as it relates to the  
22 restricted attribute;
- 23 (iii) the effectiveness of the entity’s protective security  
24 (including security governance, information security,  
25 personnel security and physical security), privacy  
26 arrangements and fraud control arrangements;
- 27 (iv) if the entity is not a participating relying party—the  
28 arrangements in place between the entity and relying  
29 parties for the protection of the restricted attribute from  
30 further disclosure;
- 31 (g) any other matter the Digital ID Regulator considers relevant.

32 *Requirement to give statement of reasons if authorisation given*

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

# EXPOSURE DRAFT

**Chapter 4** The Australian Government Digital ID System

**Part 2** The Australian Government Digital ID System

**Division 2** Participating in the Australian Government Digital ID System

## Section 64

---

1 Regulator’s website a statement of reasons for giving the  
2 authorisation.

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

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

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

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

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

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

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

21 (e) any other matter the Minister considers relevant.

## 22 **64 Variation and revocation of conditions**

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

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

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

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

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

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



# EXPOSURE DRAFT

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

## 3 **65 Applying for variation or revocation of conditions on approval**

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

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

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

## 12 **66 Notice before changes to conditions on approval**

- 13 (1) The Digital ID Regulator must not, on the Digital ID Regulator's  
14 own initiative:  
15 (a) impose a condition under subsection 62(2) on an entity's  
16 approval to participate in the Australian Government Digital  
17 ID System after the approval has been given; or  
18 (b) vary or revoke a condition imposed under subsection 64(1);  
19 unless the Digital ID Regulator has given the entity a written notice  
20 in accordance with subsection (2).
- 21 (2) The notice must:  
22 (a) state the proposed condition, variation or revocation; and  
23 (b) request the entity to give the Digital ID Regulator, within the  
24 period specified in the notice, a written statement relating to  
25 the proposed condition, variation or revocation.
- 26 (3) The Digital ID Regulator must consider any written statement  
27 given within the period specified in the notice before making a  
28 decision to:  
29 (a) impose a condition under subsection 62(2) on an entity's  
30 approval to participate in the Australian Government Digital  
31 ID System; or

# EXPOSURE DRAFT

**Chapter 4** The Australian Government Digital ID System

**Part 2** The Australian Government Digital ID System

**Division 2** Participating in the Australian Government Digital ID System

## Section 67

---

- 1 (b) vary or revoke a condition under subsection 64(1) on an  
2 entity's approval to participate in the Australian Government  
3 Digital ID System.
- 4 (4) This section does not apply if the Digital ID Regulator reasonably  
5 believes that the need to impose, vary or revoke the condition is  
6 serious and urgent.
- 7 (5) If this section does not apply to an entity because of subsection (4),  
8 the Digital ID Regulator must give a written statement of reasons  
9 to the entity as to why the Digital ID Regulator reasonably believes  
10 that the need to impose, vary or revoke the condition is serious and  
11 urgent.
- 12 (6) The statement of reasons must be given within 7 days after the  
13 condition is imposed, varied or revoked.

### 14 **67 Notice of decision of changes of conditions on approval**

- 15 (1) Subject to subsection (2), the Digital ID Regulator must give an  
16 entity written notice of a decision to impose, vary or revoke a  
17 condition on an entity's approval to participate in the Australian  
18 Government Digital ID System.
- 19 (2) The Digital ID Regulator is not required to give an entity notice of  
20 the decision if notice of the condition was given in a notice under  
21 subsection 59(5).
- 22 (3) The notice must:
- 23 (a) state the condition or the variation, or state that the condition  
24 is revoked; and
- 25 (b) state the day on which the condition, variation or revocation  
26 takes effect.

# EXPOSURE DRAFT

The Australian Government Digital ID System **Chapter 4**  
The Australian Government Digital ID System **Part 2**  
Varying, suspending and revoking approval to participate **Division 3**

Section 68

---

1 **Division 3—Varying, suspending and revoking approval to**  
2 **participate**

3 **68 Varying approval to participate in the Australian Government**  
4 **Digital ID System**

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

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

9 **69 Suspension of approval to participate in the Australian**  
10 **Government Digital ID System**

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

13 (1) The Digital ID Regulator must, in writing, suspend an approval  
14 given to an entity under section 59 if a direction under subsection  
15 60(2) is in force in relation to the entity.

16 *Digital ID Regulator may suspend approval in other circumstances*

17 (2) The Digital ID Regulator may, in writing, suspend an approval  
18 given to an entity under section 59 if:  
19 (a) the Digital ID Regulator reasonably believes that the entity  
20 has contravened or is contravening this Act; or  
21 (b) the Digital ID Regulator reasonably believes that there has  
22 been a cyber security incident involving the entity; or  
23 (c) the Digital ID Regulator reasonably believes that a cyber  
24 security incident involving the entity is imminent; or  
25 (d) the Digital ID Regulator reasonably believes that, for reasons  
26 of security (within the meaning of the *Australian Security*  
27 *Intelligence Organisation Act 1979*), including on the basis  
28 of an adverse or qualified security assessment in respect of a  
29 person, it is appropriate to do so; or

# EXPOSURE DRAFT

Chapter 4 The Australian Government Digital ID System

Part 2 The Australian Government Digital ID System

Division 3 Varying, suspending and revoking approval to participate

## Section 69

---

- 1 (e) if the entity is a body corporate—the entity is a Chapter 5  
2 body corporate (within the meaning of the *Corporations Act*  
3 *2001*); or  
4 (f) if the entity is an individual—the entity is an insolvent under  
5 administration; or  
6 (g) the Digital ID Regulator is satisfied that it is not appropriate  
7 for the entity to participate in the Australian Government  
8 Digital ID System; or  
9 (h) circumstances specified in the Digital ID Rules apply in  
10 relation to the entity.

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

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

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

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

23 *Digital ID Regulator may suspend approval on application*

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

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

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

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

- 32 (7) The show cause notice must:

# EXPOSURE DRAFT

The Australian Government Digital ID System **Chapter 4**  
The Australian Government Digital ID System **Part 2**  
Varying, suspending and revoking approval to participate **Division 3**

## Section 69

---

- 1 (a) state the grounds on which the Digital ID Regulator proposes  
2 to suspend the entity's approval; and  
3 (b) invite the entity to give the Digital ID Regulator, within 28  
4 days after the day the notice is given, a written statement  
5 showing cause why the Digital ID Regulator should not  
6 suspend the approval.

7 *Exception—cyber security incident or security*

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

10 *Notice of suspension*

- 11 (9) If the Digital ID Regulator suspends an entity's approval under  
12 subsection (1), (2) or (5), the Digital ID Regulator must give the  
13 entity a written notice stating the following:  
14 (a) that the entity's approval to participate in the Australian  
15 Government Digital ID System is suspended;  
16 (b) the reasons for the suspension;  
17 (c) the day the suspension is to start;  
18 (d) if the approval is suspended for a period—the period of the  
19 suspension;  
20 (e) if the approval is suspended until a specified event occurs or  
21 action is taken—the event or action;  
22 (f) if the approval is suspended indefinitely—that fact.

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

29 *Revocation of suspension*

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

# EXPOSURE DRAFT

**Chapter 4** The Australian Government Digital ID System

**Part 2** The Australian Government Digital ID System

**Division 3** Varying, suspending and revoking approval to participate

## Section 70

---

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

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

6 *Effect of suspension*

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

## 11 **70 Revocation of approval to participate in the Australian** 12 **Government Digital ID System**

13 *Digital ID Regulator may revoke approval*

- 14 (1) The Digital ID Regulator may, in writing, revoke an approval  
15 given to an entity under section 59 if:
- 16 (a) the Digital ID Regulator reasonably believes that the entity  
17 has contravened or is contravening this Act; or
  - 18 (b) the Digital ID Regulator reasonably believes that there has  
19 been a cyber security incident involving the entity; or
  - 20 (c) the Digital ID Regulator reasonably believes that, for reasons  
21 of security (within the meaning of the *Australian Security*  
22 *Intelligence Organisation Act 1979*), including on the basis  
23 of an adverse or qualified security assessment in respect of a  
24 person, it is appropriate to do so; or
  - 25 (d) if the entity is a body corporate—the entity is a Chapter 5  
26 body corporate (within the meaning of the *Corporations Act*  
27 *2001*); or
  - 28 (e) if the entity is an individual—the entity is an insolvent under  
29 administration; or
  - 30 (f) the Digital ID Regulator is satisfied that it is not appropriate  
31 for the entity to participate in the Australian Government  
32 Digital ID System; or

# EXPOSURE DRAFT

The Australian Government Digital ID System **Chapter 4**  
The Australian Government Digital ID System **Part 2**  
Varying, suspending and revoking approval to participate **Division 3**

## Section 70

---

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

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

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

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

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

### 15 *Revocation on application*

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

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

### 20 *Show cause notice must generally be given before decision to* 21 *revoke*

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

25 (6) The show cause notice must:

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

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

# EXPOSURE DRAFT

**Chapter 4** The Australian Government Digital ID System

**Part 2** The Australian Government Digital ID System

**Division 3** Varying, suspending and revoking approval to participate

## Section 70

---

1

### *Notice of revocation*

2

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

3

4

5

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

6

7

(b) the reasons for the revocation;

8

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

9

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

10

11

12

13

14

15

### *Approval can be revoked even while suspended*

16

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

17

18

19



# EXPOSURE DRAFT

The Australian Government Digital ID System **Chapter 4**  
The Australian Government Digital ID System **Part 2**  
Other matters relating to the Australian Government Digital ID System **Division 4**

Section 71

---

1 **Division 4—Other matters relating to the Australian**  
2 **Government Digital ID System**

3 **71 Creating and using a digital ID is voluntary**

4 *Creating and using a digital ID is voluntary*

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

8 *Exceptions*

9 (2) Subsection (1) does not apply to a service of a participating relying  
10 party if:  
11 (a) the service provides access to another service; and  
12 (b) the individual can access the other service without creating or  
13 using a digital ID through the Australian Government Digital  
14 ID System.

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

23 (3) Subsection (1) does not apply if:  
24 (a) a law of the Commonwealth, a State or a Territory requires  
25 verification of the individual's identity solely by means of a  
26 digital ID; or  
27 (b) the participating relying party is providing a service, or  
28 access to a service, to an individual who is acting on behalf  
29 of another entity in a professional or business capacity;  
30 (c) the participating relying party holds an exemption under  
31 subsection (4).

# EXPOSURE DRAFT

**Chapter 4** The Australian Government Digital ID System

**Part 2** The Australian Government Digital ID System

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

## Section 71

---

1

### *Exemptions*

2

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

3

4

5

6

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

7

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

8

9

10

11

12

13

14

(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.

15

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

16

17

18

19

20

21

22

23

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

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

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

24

- (7) An exemption under subsection (4):

25

26

27

(a) must be in writing; and

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

28

- (8) The Digital ID Regulator must:

29

30

31

32

(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.

# EXPOSURE DRAFT

1     **72 Notice before exemption is revoked**

- 2             (1) The Digital ID Regulator must not revoke an exemption granted to  
3                 an entity under subsection 71(3) unless the Digital ID Regulator  
4                 has given the entity a written notice in accordance with  
5                 subsection (2).
- 6             (2) The notice must:
- 7                 (a) state that the Digital ID Regulator proposes to revoke the  
8                     exemption; and
- 9                 (b) give reasons for the proposed revocation; and
- 10                (c) request the entity to give the Digital ID Regulator, within the  
11                    period specified in the notice, a written statement relating to  
12                    the proposed revocation.
- 13             (3) The Digital ID Regulator must consider any written statement  
14                 given within the period specified in the notice before making a  
15                 decision to revoke the exemption.
- 16             (4) This section does not apply if the Digital ID Regulator reasonably  
17                 believes that the need to revoke the exemption is serious and  
18                 urgent.

19     **73 Holding etc. information outside Australia**

- 20             (1) The Digital ID Rules may make provision in relation to the  
21                 holding, storing, handling or transfer of information outside  
22                 Australia if the information is or was generated, collected, held or  
23                 stored by accredited entities within the Australian Government  
24                 Digital ID System.
- 25             (2) Without limiting subsection (1), the Digital ID Rules may:
- 26                 (a) prohibit (either absolutely or unless particular circumstances  
27                     are met or conditions are complied with) the holding, storing,  
28                     handling or transferring of such information outside  
29                     Australia; and
- 30                 (b) empower the Digital ID Regulator to grant exemptions to  
31                     entities from any such prohibitions; and
- 32                 (c) may be expressed to apply to:

# EXPOSURE DRAFT

Chapter 4 The Australian Government Digital ID System

Part 2 The Australian Government Digital ID System

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

## Section 74

---

- 1 (i) entities that hold an approval to participate in the  
2 Australian Government Digital ID System; or  
3 (ii) entities whose approval to participate in the Australian  
4 Government Digital ID System is suspended; or  
5 (iii) entities whose approval to participate in the Australian  
6 Government Digital ID System has been revoked.
- 7 (3) An entity is liable to a civil penalty if:  
8 (a) the entity is subject to a requirement under the Digital ID  
9 Rules made for the purposes of subsection (1); and  
10 (b) the entity fails to comply with the requirement.
- 11 Civil penalty: 300 penalty units.

## 74 Reportable incidents

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

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

- 20 (2) Without limiting subsection (1), the Digital ID Rules may make  
21 provision in relation to the following matters:  
22 (a) the entities that are covered by the arrangements;  
23 (b) the kinds of incidents that must be notified;  
24 (c) the information that must be included in notification about  
25 reportable incidents;  
26 (d) the manner in which and period within which reportable  
27 incidents must be notified to the Digital ID Regulator;  
28 (e) action that must be taken in relation to reportable incidents;  
29 (f) how the Digital ID Regulator deals with reportable incidents,  
30 including action that may be taken by the Digital ID  
31 Regulator in dealing with a reportable incident such as:  
32 (i) requiring an entity to do something; or

# EXPOSURE DRAFT

- 1 (ii) authorising the provision of information relating to  
2 reportable incidents by the Digital ID Regulator to the  
3 Minister, the Information Commissioner, accredited  
4 entities, participating relying parties or other specified  
5 bodies;
- 6 (g) authorising the collection of information relating to  
7 reportable incidents by the Minister, the Information  
8 Commissioner, accredited entities, participating relying  
9 parties or other specified bodies.
- 10 (3) Without limiting paragraph (2)(b), the Digital ID Rules may  
11 specify the following kinds of incidents:
- 12 (a) digital ID fraud incidents;  
13 (b) cyber security incidents;  
14 (c) changes in control (within the meaning of section 910B of  
15 the *Corporations Act 2001*) of entities covered by the  
16 arrangements;  
17 (d) if an accredited entity engages contractors to provide an  
18 accredited service, or part of an accredited service, of the  
19 entity—changes in relation to such contractors.
- 20 (4) An entity is liable to a civil penalty if:
- 21 (a) the entity is subject to a requirement under the Digital ID  
22 Rules made for the purposes of subsection (1); and  
23 (b) the entity fails to comply with the requirement.
- 24 Civil penalty: 300 penalty units.

## 75 Interoperability

- 26 (1) The Digital ID Rules may provide for or in relation to requirements  
27 relating to the interoperability obligation within the Australian  
28 Government Digital ID System.
- 29 (2) For the purposes of subsection (1), the *interoperability obligation*  
30 means:
- 31 (a) the obligation on participating relying parties to provide  
32 individuals with a choice of accredited identity service

# EXPOSURE DRAFT

**Chapter 4** The Australian Government Digital ID System

**Part 2** The Australian Government Digital ID System

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

## Section 75

---

- 1 providers when the individual seeks to verify their identity or  
2 authenticate their digital ID or other information; and
- 3 (b) the obligation on accredited entities participating in the  
4 Australian Government Digital ID System to provide their  
5 accredited services to other entities participating in the  
6 system.
- 7 (3) Without limiting subsection (1), the Digital ID Rules may do any  
8 of the following:
- 9 (a) specify the circumstances in which the interoperability  
10 obligation applies to participating relying parties and  
11 accredited entities;
- 12 (b) provide for the Minister, on application, to grant exemptions  
13 from the interoperability obligation;
- 14 (c) specify the grounds on which the Minister may grant  
15 exemptions, which may include the following:
- 16 (i) that the Minister is satisfied that a service, or access to a  
17 service, provided by a participating relying party that is  
18 a government entity is of a kind that should be provided  
19 only to other government entities;
- 20 (ii) that the participating relying party provides a service, or  
21 access to a service, that the Minister is satisfied is of a  
22 kind that would promote use of digital IDs if the  
23 service, or access to the service, was available through  
24 the Australian Government Digital ID System;
- 25 (iii) that the exemption is of a limited duration to allow for  
26 the implementation of required business practices or  
27 technological systems, or to facilitate the use of the  
28 Australian Government Digital ID System by particular  
29 kinds of entities;
- 30 (iv) that an entity will provide an arrangement to assist  
31 individuals who would otherwise be at a disadvantage in  
32 accessing the Australian Government Digital ID  
33 System;
- 34 (v) the exemption is necessary to satisfy the requirements of  
35 another legislative provision or scheme;

# EXPOSURE DRAFT

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

## 4 **76 Service levels for accredited entities and participating relying** 5 **parties**

- 6 (1) The Digital ID Standards Chair may, in writing, determine either or  
7 both of the following:  
8 (a) service levels relating to the availability and performance of  
9 the information technology systems through which accredited  
10 entities that hold an approval to participate in the Australian  
11 Government Digital ID System will provide their accredited  
12 services;  
13 (b) service levels relating to the availability and performance of  
14 the services participating relying parties are approved to  
15 provide, or provide access to, within the Australian  
16 Government Digital ID System.  
17 (2) A determination made under subsection (1) is a legislative  
18 instrument, but section 42 (disallowance) of the *Legislation Act*  
19 *2003* does not apply to the instrument.

## 20 **77 Entities may conduct testing in relation to the Australian** 21 **Government Digital ID System**

- 22 (1) The Digital ID Regulator may authorise an entity to conduct testing  
23 in relation to the Australian Government Digital ID System for the  
24 purposes of determining the entity's capability or suitability to  
25 participate in the system.  
26 (2) The authorisation:  
27 (a) must be in writing; and  
28 (b) must specify the period for which it is in force, which must  
29 not exceed 3 months; and  
30 (c) may be granted unconditionally or subject to conditions.  
31 Note: The Digital ID Regulator may vary or revoke the authorisation: see  
32 subsection 33(3) of the *Acts Interpretation Act 1901*.

# EXPOSURE DRAFT

**Chapter 4** The Australian Government Digital ID System

**Part 2** The Australian Government Digital ID System

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

## Section 78

---

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

### 4                   **78 Use and disclosure of personal information to conduct testing**

- 5                   (1) An accredited entity may use or disclose personal information of  
6                   an individual if:  
7                   (a) the accredited entity uses or discloses the information for the  
8                   purposes of conducting testing in relation to the Australian  
9                   Government Digital ID System; and  
10                  (b) the accredited entity or another entity is authorised under  
11                  section 77 to conduct the testing using the information; and  
12                  (c) the individual to whom the information relates has expressly  
13                  consented to the use or disclosure of the information for that  
14                  purpose.  
15                  (2) This section applies despite anything else in this Act.



# EXPOSURE DRAFT

The Australian Government Digital ID System **Chapter 4**

Liability and redress framework **Part 3**

Liability of participating entities **Division 1**

Section 79

---

1 **Part 3—Liability and redress framework**

2 **Division 1—Liability of participating entities**

3 **79 Accredited entities participating in the Australian Government**  
4 **Digital ID System protected from liability in certain**  
5 **circumstances**

- 6 (1) This section applies if, while participating in the Australian  
7 Government Digital ID System, an accredited entity:
- 8 (a) provides, or fails to provide, an accredited service of the  
9 entity to another accredited entity participating in the  
10 Australian Government Digital ID System, or to a  
11 participating relying party; and
  - 12 (b) provides, or fails to provide, the accredited service in good  
13 faith, in compliance with this Act.
- 14 (2) The accredited entity is not liable to any action or other  
15 proceeding, whether civil or criminal, in relation to that accredited  
16 service or the provision of that accredited service.
- 17 (3) An entity that wishes to rely on subsection (2) in relation to an  
18 action or other proceeding bears an evidential burden (within the  
19 meaning of the Regulatory Powers Act) in relation to that matter.

# EXPOSURE DRAFT

Chapter 4 The Australian Government Digital ID System

Part 3 Liability and redress framework

Division 2 Statutory contract

Section 80

---

1 **Division 2—Statutory contract**

2 **80 Statutory contract between entities participating in the**  
3 **Australian Government Digital ID System**

- 4 (1) A contract is taken to be in force between:  
5 (a) an accredited entity and each other accredited entity; and  
6 (b) an accredited entity and each participating relying party;  
7 under which each accredited entity agrees to:  
8 (c) provide the entity's accredited services while participating in  
9 the Australian Government Digital ID System in compliance  
10 with this Act, to the extent it relates to verifying the identity  
11 of an individual or authenticating the digital ID of, or  
12 information about, an individual; and  
13 (d) comply with requirements in relation to intellectual property  
14 rights that are prescribed by the Digital ID Rules for the  
15 purposes of this paragraph.

16 Note 1: This means an accredited entity will be taken to have a separate  
17 contract with each other accredited entity and with each participating  
18 relying party.

19 Note 2: The Digital ID Rules may provide that some provisions of this Act  
20 (which is defined to include the Digital ID Data Standards and other  
21 legislative instruments) are not covered by the contract (see  
22 subsection (5)).

- 23 (2) The contract is taken to be in force during the period:  
24 (a) starting on the day that the participation start day for both  
25 entities has arrived or passed; and  
26 (b) ending on the day on which the approval to participate in the  
27 Australian Government Digital ID System has been revoked  
28 for one or both of the entities.
- 29 (3) If an accredited entity breaches the contract, an application to the  
30 Federal Circuit and Family Court of Australia (Division 2) may be  
31 made by the party to the contract that has suffered, or is likely to  
32 suffer, loss or damage as a result of the breach.

# EXPOSURE DRAFT

The Australian Government Digital ID System **Chapter 4**

Liability and redress framework **Part 3**

Statutory contract **Division 2**

## Section 81

---

- 1 (4) After giving an opportunity to be heard to the applicant and the  
2 entity (the *respondent*) against whom the order is sought, the  
3 Federal Circuit and Family Court of Australia (Division 2) may  
4 make any or all of the following orders:  
5 (a) an order giving directions to the respondent about  
6 compliance with, or enforcement of, the contract;  
7 (b) an order directing the respondent to compensate the entity  
8 that has suffered loss or damage as a result of the breach;  
9 (c) an order directing the respondent to prevent or reduce loss or  
10 damage suffered, or likely to be suffered;  
11 (d) any other order that the Court considers appropriate.
- 12 (5) The Digital ID Rules may make provision in relation to the  
13 following matters:  
14 (a) conduct or circumstances that do, or do not, constitute  
15 breaches of contract;  
16 (b) provision of this Act that are not covered by the contract;  
17 (c) limits on the kinds of losses or damages for which  
18 compensation may be payable;  
19 (d) limits on the amount of compensation that an accredited  
20 entity may be liable to pay.

### 21 **81 Participating entities to maintain insurance as directed by Digital** 22 **ID Regulator**

- 23 (1) The Digital ID Regulator may, in writing, direct an accredited  
24 entity that is participating in the Australian Government Digital ID  
25 System to maintain adequate insurance against any liabilities  
26 arising in connection with the obligations under section 80.
- 27 (2) If the Digital ID Regulator gives a direction to an entity under  
28 subsection (1), the direction is taken to be a condition imposed  
29 under subsection 62(2) on the entity's approval to participate in the  
30 Australian Government Digital ID System.
- 31 (3) A direction given under this section is not a legislative instrument.

# EXPOSURE DRAFT

**Chapter 4** The Australian Government Digital ID System

**Part 3** Liability and redress framework

**Division 2** Statutory contract

Section 82

---

1 **82 Dispute resolution procedures**

2           The Digital ID Rules may make provision for and in relation to  
3           dispute resolution procedures that must be complied with before an  
4           entity can apply for an order under subsection 80(3).

# EXPOSURE DRAFT

The Australian Government Digital ID System **Chapter 4**

Liability and redress framework **Part 3**

Redress framework **Division 3**

Section 83

---

1 **Division 3—Redress framework**

2 **83 Redress framework**

- 3 (1) The Digital ID Rules may provide for or in relation to a redress  
4 framework for incidents that occur in relation to accredited  
5 services of accredited entities that are provided within the  
6 Australian Government Digital ID System.
- 7 (2) Without limiting subsection (1), the redress framework may deal  
8 with the following matters:
- 9 (a) the entities that are covered by the framework;
  - 10 (b) the kinds of incidents that are covered by the framework,  
11 which may include digital ID fraud incidents and cyber  
12 security incidents;
  - 13 (c) procedures for dealing with incidents that are covered by the  
14 framework;
  - 15 (d) requirements relating to notifying entities affected by  
16 incidents covered by the framework;
  - 17 (e) the provision of information, support and assistance to  
18 entities affected by incidents covered by the framework;
  - 19 (f) development and publication of policies relating to the  
20 identification, management and resolution of incidents  
21 covered by the framework.

# EXPOSURE DRAFT

**Chapter 5** Digital ID Regulator

**Part 1** Introduction

Section 84

---

1 **Chapter 5—Digital ID Regulator**

2 **Part 1—Introduction**

3

4 **84 Simplified outline of this Chapter**

1 **Part 2—Digital ID Regulator**  
2

3 **85 Digital ID Regulator**

4 The Digital ID Regulator is the Australian Competition and  
5 Consumer Commission.

6 Note: The Australian Competition and Consumer Commission is established  
7 by Part II of the *Competition and Consumer Act 2010*.

8 **86 Functions of the Digital ID Regulator**

9 *Consultation note:*

10 The Bill will set out the functions of the Digital ID Regulator.  
11 These functions primarily relate to the regulation of accredited  
12 entities and other entities participating as relying parties in the  
13 Australian Government Digital ID System. The Bill sets out other  
14 more operational functions relating to ensuring the integrity and  
15 performance of the Australian Government Digital ID System  
16 which are currently performed by Services Australia.

17 The sharing of these functions between the Digital ID Regulator  
18 and Services Australia remains under consideration.

19 Below is a description of the current intention for the sharing of  
20 functions between Australian Competition and Consumer  
21 Commission as the Digital ID Regulator and the Chief Executive  
22 Officer of Services Australia as administrator of the Australian  
23 Government Digital ID System.

24 Digital ID Regulator:

- 25 · the functions conferred on the Digital ID Regulator by or  
26 under the Act involving accreditation, approvals to participate  
27 in the Australian Government Digital ID System and

# EXPOSURE DRAFT

Chapter 5 Digital ID Regulator

Part 2 Digital ID Regulator

## Section 87

---

- 1 enforcement, other than where those functions are conferred  
2 on Services Australia
- 3 · advising the Finance Minister on matters relating to any of the  
4 Digital ID Regulator's functions
- 5 · anything that is incidental or conducive to the performance of  
6 any of the above functions.
- 7 Services Australia: administering the operation of the Australian  
8 Government Digital ID System:
- 9 · identifying and managing risks in relation to the Australian  
10 Government Digital ID System
- 11 · managing Digital ID fraud incidents and cyber security  
12 incidents that affect the Australian Government Digital ID  
13 System
- 14 · advising the Finance Minister or the Digital ID Regulator on  
15 matters relating to the operation of the Australian Government  
16 Digital ID System
- 17 · anything that is incidental or conducive to the performance of  
18 any of the above functions.

### 19 **87 Powers of the Digital ID Regulator**

20 The Digital ID Regulator has power to do all things necessary or  
21 convenient to be done for or in connection with the performance of  
22 the Regulator's functions under this Act.



# EXPOSURE DRAFT

Digital ID Regulator **Chapter 5**

Digital ID Regulator **Part 2**

Confidentiality obligations of the Digital ID Regulator and certain other persons

**Division 2**

Section 88

---

1 **Division 2—Confidentiality obligations of the Digital ID**  
2 **Regulator and certain other persons**

3 **88 Prohibition on entrusted persons using or disclosing personal or**  
4 **commercially sensitive information**

5 *Offence*

- 6 (1) A person commits an offence if:  
7 (a) the person is or has been an entrusted person; and  
8 (b) the person obtains protected information in the course of, or  
9 for the purposes of, performing functions or exercising  
10 powers under this Act; and  
11 (c) the person uses or discloses the information; and  
12 (d) either of the following applies:  
13 (i) the information is personal information about an  
14 individual;  
15 (ii) there is a risk that the use or disclosure might  
16 substantially prejudice the commercial interests of  
17 another person.

18 Penalty: Imprisonment for 2 years or 120 penalty units, or both.

- 19 (2) An *entrusted person* means:  
20 (a) the Digital ID Regulator; or  
21 (b) a member of the Commission (within the meaning of the  
22 *Competition and Consumer Act 2010*); or  
23 (c) an associate member of the Australian Competition and  
24 Consumer Commission; or  
25 (d) a member of the staff of the Australian Competition and  
26 Consumer Commission; or  
27 (e) a person engaged under section 27A of the *Competition and*  
28 *Consumer Act 2010*.

# EXPOSURE DRAFT

Chapter 5 Digital ID Regulator

Part 2 Digital ID Regulator

Division 2 Confidentiality obligations of the Digital ID Regulator and certain other persons

## Section 89

---

1

*Exception—authorised use or disclosure*

2

- (3) Subsection (1) does not apply if the use or disclosure is authorised by section 89 (authorised uses and disclosures).

3

4

Note: A defendant bears an evidential burden in relation to a matter in this subsection (see subsection 13.3(3) of the *Criminal Code*).

5

6

*Definition of protected information*

7

- (4) **Protected information** means information that was disclosed or obtained under or for the purposes of this Act.

8

9

## **89 Authorised uses and disclosures of personal or commercially sensitive information by entrusted persons**

10

11

- (1) An entrusted person may use or disclose protected information if:

12

- (a) the use or disclosure is made for the purposes of:

13

- (i) performing a duty or function, or exercising a power, under or in relation to this Act; or

14

15

- (ii) enabling another person to perform duties or functions, or exercise powers, under or in relation to this Act; or

16

17

- (iii) assisting in the administration or enforcement of another law of the Commonwealth, or of a State or Territory; or

18

19

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

20

- (i) a law of the Commonwealth (including this Act); or

21

- (ii) a law of a State or Territory that is prescribed by the Digital ID Rules; or

22

23

- (c) the person referred to in subparagraph 88(1)(d)(i) or (ii) has expressly consented to the use or disclosure; or

24

25

- (d) at the time of the use or disclosure, the protected information is already lawfully publicly available; or

26

27

- (e) both:

28

- (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

29

30

- (ii) the use or disclosure is made in accordance with any requirements prescribed by the Digital ID Rules; or

31

32

# EXPOSURE DRAFT

Digital ID Regulator **Chapter 5**

Digital ID Regulator **Part 2**

Confidentiality obligations of the Digital ID Regulator and certain other persons

**Division 2**

## Section 90

---

- 1 (f) both:
- 2 (i) the entrusted person believes on reasonable grounds that
- 3 the use or disclosure is necessary to prevent or lessen a
- 4 serious and imminent threat to the life or health of a
- 5 person; and
- 6 (ii) the use or disclosure is for the purposes of preventing or
- 7 lessening that threat.
- 8 (2) An instrument made under subparagraph (1)(e)(i) certifying that a
- 9 particular use or disclosure is in the public interest is not a
- 10 legislative instrument.
- 11 (3) An instrument made under subparagraph (1)(e)(i) certifying that a
- 12 kind of use or disclosure is in the public interest is a legislative
- 13 instrument.

### **90 Disclosing personal or commercially sensitive information to courts and tribunals etc. by entrusted persons**

- 14
- 15
- 16 (1) Except where it is necessary to do so for the purposes of giving
- 17 effect to this Act, an entrusted person is not to be required:
- 18 (a) to produce a document containing protected information to a
- 19 body mentioned in subsection (2); or
- 20 (b) to disclose protected information to such a body;
- 21 if either of the following applies:
- 22 (c) the information is personal information of an individual other
- 23 than the entrusted person;
- 24 (d) there is a risk that production of the document or disclosure
- 25 of the information might substantially prejudice the
- 26 commercial interests of a person.
- 27 (2) The bodies are a court, tribunal, authority or other person having
- 28 power to require the production of documents or the answering of
- 29 questions.

# EXPOSURE DRAFT

## Section 91

---

### Part 2—Advisory committees

#### 91 Advisory committees

- (1) The Minister may establish, in writing, such advisory committees as the Minister considers appropriate to provide advice to the following in relation to the performance of the Digital ID Regulator’s functions and exercise of the Regulator’s powers under this Act:
  - (a) the Minister;
  - (b) the Secretary;
  - (c) the Digital ID Data Standards Chair.
- (2) An advisory committee is to consist of such persons as the Minister determines.
- (3) If the Minister establishes an advisory committee under subsection (1), the Minister must, in writing, determine:
  - (a) the committee’s terms of reference; and
  - (b) the terms and conditions of appointment of the members of the committee, including:
    - (i) term of office; and
    - (ii) remuneration; and
    - (iii) allowances; and
    - (iv) leave of absence; and
    - (v) disclosure of interests; and
    - (vi) termination of membership; and
  - (c) the procedures to be followed by the committee.
- (4) An instrument made under subsection (1) or (3) is not a legislative instrument.

# EXPOSURE DRAFT

Digital ID Data Standards **Chapter 6**  
Introduction **Part 1**

Section 92

---

1 **Chapter 6—Digital ID Data Standards**

2 **Part 1—Introduction**

3

4 **92 Simplified outline of this Chapter**

**EXPOSURE DRAFT**

# EXPOSURE DRAFT

## Part 2—Digital ID Data Standards

### 93 Digital ID Data Standards

- (1) The Digital ID Standards Chair may, in writing, make one or more standards (*Digital ID Data Standards*) about the following:
  - (a) technical integration requirements for entities to participate in the Australian Government Digital ID System;
  - (b) technical or design features that entities must have to participate in the Australian Government Digital ID System;
  - (c) if required to do so by the Accreditation Rules—technical, data or design standards, including test standards for an entity’s information technology systems, relating to accreditation;
  - (d) other matters prescribed by the Digital ID Rules.
- (2) Without limiting subsection 33(3A) of the *Acts Interpretation Act 1901*, Digital ID Data Standards may provide differently for different kinds of entities, things or circumstances.
- (3) Digital ID Data Standards that are inconsistent with the Accreditation Rules have no effect to the extent of the inconsistency, but Digital ID Data Standards are taken to be consistent with the Accreditation Rules to the extent that Digital ID Data Standards are capable of operating concurrently with the Accreditation Rules.
- (4) Digital ID Data Standards are legislative instruments, but section 42 (disallowance) of the *Legislation Act 2003* does not apply to them.

### 94 Requirement to consult before making

- (1) Before making or amending Digital ID Data Standards under section 93, the Digital ID Data Standards Chair must:
  - (a) consult the Minister;

# EXPOSURE DRAFT

## Section 94

---

- 1 (b) cause to be published on the Department’s website a notice:  
2 (i) setting out the draft standards or amendments; and  
3 (ii) inviting persons to make submissions to the Chair about  
4 the draft standards or amendments within the period  
5 specified in the notice (which must be at least 28 days  
6 after the notice is published); and  
7 (c) consider any submissions received within the specified  
8 period.
- 9 (2) The Digital ID Data Standards Chair may consider any  
10 submissions received after the specified period if the Chair  
11 considers it appropriate to do so.
- 12 (3) Before making or amending Digital ID Data Standards under  
13 section 93, the Digital ID Data Standards Chair may consult:  
14 (a) the Digital ID Regulator; or  
15 (b) the Information Commissioner.
- 16 (4) This section does not limit section 17 of the *Legislation Act 2003*  
17 (rule-makers should consult before making legislative instrument).

# EXPOSURE DRAFT

Chapter 6 Digital ID Data Standards

Part 3 Digital ID Data Standards Chair

Division 1 Establishment and functions of the Digital ID Data Standards Chair

Section 95

---

1 **Part 3—Digital ID Data Standards Chair**

2 **Division 1—Establishment and functions of the Digital ID**  
3 **Data Standards Chair**

4 **95 Data Standards Chair**

5 There is to be a Digital ID Data Standards Chair.

6 **96 Functions of the Digital ID Data Standards Chair**

7 The functions of the Digital ID Data Standards Chair are:

- 8 (a) to make Digital ID Data Standards; and  
9 (b) to review those standards regularly; and  
10 (c) such other functions as are conferred on the Chair by this  
11 Act; and  
12 (d) to do anything incidental or conducive to the performance of  
13 any of the above functions.

14 **97 Powers of the Digital ID Data Standards Chair**

15 The Digital ID Data Standards Chair has the power to do all things  
16 necessary or convenient to be done for or in connection with the  
17 performance of the Chair's functions.

18 **98 Directions to the Digital ID Data Standards Chair**

- 19 (1) The Minister may give written directions to the Digital ID Data  
20 Standards Chair about the performance of the Chair's functions  
21 and the exercise of the Chair's powers.  
22 (2) A direction under subsection (1) must be of a general nature only.  
23 (3) The Digital ID Data Standards Chair must comply with a direction  
24 under subsection (1).  
25 (4) A direction under subsection (1) is not a legislative instrument.



# EXPOSURE DRAFT

1 **Division 2—Appointment of the Digital ID Data Standards**  
2 **Chair**

3 **99 Appointment**

4 (1) The Digital ID Data Standards Chair is to be appointed by the  
5 Minister by written instrument.

6 Note: The Minister will be the Digital ID Data Standards Chair in the  
7 absence of an appointment under this section (see the definition of  
8 *Digital ID Data Standards Chair* in section 9).

9 (2) The Digital ID Data Standards Chair is to be appointed on a  
10 full-time or part-time basis.

11 **100 Term of appointment**

12 The Digital ID Data Standards Chair holds office for the period  
13 specified in the instrument of appointment. The period must not  
14 exceed 3 years.

15 Note: The Digital ID Data Standards Chair may be reappointed: see  
16 section 33AA of the *Acts Interpretation Act 1901*.

17 **101 Acting appointments**

18 The Minister may, by written instrument, appoint a person to act as  
19 the Digital ID Data Standards Chair:

20 (a) during a vacancy in the office of Digital ID Data Standards  
21 Chair (whether or not an appointment has previously been  
22 made to the office); or

23 (b) during any period, or during all periods, when the Digital ID  
24 Data Standards Chair:

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

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

28 Note: For rules that apply to acting appointments, see sections 33AB and  
29 33A of the *Acts Interpretation Act 1901*.

# EXPOSURE DRAFT

Chapter 6 Digital ID Data Standards

Part 3 Digital ID Data Standards Chair

Division 2 Appointment of the Digital ID Data Standards Chair

## Section 102

---

1 **102 Application of the finance law etc.**

2 (1) For the purposes of the finance law (within the meaning of the  
3 *Public Governance, Performance and Accountability Act 2013*),  
4 the Digital ID Data Standards Chair is an official of the  
5 Department.

6 Note: A consequence of this subsection is that the Secretary of the  
7 Department is the accountable authority (within the meaning of that  
8 Act) applicable to the Digital ID Data Standards Chair.

9 (2) The Secretary of the Department, when preparing the Department's  
10 annual report under section 46 of the *Public Governance,*  
11 *Performance and Accountability Act 2013* for a period, must  
12 include information in that report about:

13 (a) the performance of the Digital ID Data Standards Chair's  
14 functions; and

15 (b) the exercise of the Digital ID Data Standards Chair's powers;  
16 during the period.

17 (3) If at any time the Digital ID Data Standards Chair is the Minister  
18 then:

19 (a) subsections (1) and (2) do not apply during that time; and

20 (b) the Department's annual report under section 46 of the  
21 *Public Governance, Performance and Accountability Act*  
22 *2013* for the period that includes that time must include  
23 information about the performance of the Digital ID Data  
24 Standards Chair's functions, and the exercise of the Digital  
25 ID Data Standards Chair's powers, at that time.

# EXPOSURE DRAFT

1 **Division 3—Terms and conditions for the Digital ID Data**  
2 **Standards Chair**

3 **103 Remuneration**

- 4 (1) The Digital ID Data Standards Chair is to be paid the remuneration  
5 that is determined by the Remuneration Tribunal. If no  
6 determination of that remuneration by the Tribunal is in operation,  
7 the Digital ID Data Standards Chair is to be paid the remuneration  
8 that is prescribed by legislative instrument under subsection (3).
- 9 (2) The Digital ID Data Standards Chair is to be paid the allowances  
10 that are prescribed by legislative instrument under subsection (3).
- 11 (3) The Minister may, by legislative instrument, prescribe:  
12 (a) remuneration for the purposes of subsection (1); and  
13 (b) allowances for the purposes of subsection (2).
- 14 (4) Subsections (1) and (2) do not apply while the Digital ID Data  
15 Standards Chair is the Minister.
- 16 (5) Subsections 7(9) and (13) of the *Remuneration Tribunal Act 1973*  
17 do not apply in relation to the office of the Digital ID Data  
18 Standards Chair.
- 19 Note: The effect of this subsection is that remuneration or allowances of the  
20 Digital ID Data Standards Chair will be paid out of money  
21 appropriated by an Act other than the *Remuneration Tribunal Act*  
22 *1973*.
- 23 (6) This section has effect subject to the *Remuneration Tribunal Act*  
24 *1973* (except as provided by subsection (5) of this section).

25 **104 Leave of absence**

- 26 (1) If the Digital ID Data Standards Chair is appointed on a full-time  
27 basis, the Data Standards Chair has the recreation leave  
28 entitlements that are determined by the Remuneration Tribunal.

# EXPOSURE DRAFT

Chapter 6 Digital ID Data Standards

Part 3 Digital ID Data Standards Chair

Division 3 Terms and conditions for the Digital ID Data Standards Chair

## Section 105

---

- 1 (2) If the Digital ID Data Standards Chair is appointed on a full-time  
2 basis, the Minister may grant the Data Standards Chair leave of  
3 absence, other than recreation leave, on the terms and conditions as  
4 to remuneration or otherwise that the Minister determines.
- 5 (3) If the Digital ID Data Standards Chair is appointed on a part-time  
6 basis, the Secretary of the Department may grant leave of absence  
7 to the Data Standards Chair on the terms and conditions that the  
8 Secretary determines.

### 9 **105 Outside work**

10 The Digital ID Data Standards Chair must not engage in paid work  
11 outside the duties of the Digital ID Data Standards Chair's office  
12 without the Minister's approval.

### 13 **106 Disclosure of interests**

- 14 (1) The Digital ID Data Standards Chair must give written notice to  
15 the Minister of any direct or indirect pecuniary interest that the  
16 Digital ID Data Standards Chair has or acquires and that conflicts  
17 or could conflict with the proper performance of the Digital ID  
18 Data Standards Chair's functions.
- 19 (2) Subsection (1) applies in addition to section 29 of the *Public*  
20 *Governance, Performance and Accountability Act 2013* (which  
21 deals with the duty to disclose interests).

### 22 **107 Resignation of appointment**

#### 23 *Resignation*

- 24 (1) The Digital ID Data Standards Chair may resign the Digital ID  
25 Data Standards Chair's appointment by giving the Minister a  
26 written resignation.
- 27 (2) The resignation takes effect on the day it is received by the  
28 Minister or, if a later day is specified in the resignation, on that  
29 later day.

# EXPOSURE DRAFT

## 108 Termination of appointment

- 1
- 2 (1) The Minister may terminate the appointment of the Digital ID Data  
3 Standards Chair:
- 4 (a) for misbehaviour; or  
5 (b) if the Digital ID Data Standards Chair is unable to perform  
6 the duties of the Digital ID Data Standards Chair's office  
7 because of physical or mental incapacity.
- 8 (2) The Minister may terminate the appointment of the Digital ID Data  
9 Standards Chair if:
- 10 (a) the Digital ID Data Standards Chair:
- 11 (i) becomes bankrupt; or  
12 (ii) applies to take the benefit of any law for the relief of  
13 bankrupt or insolvent debtors; or  
14 (iii) compounds with the Digital ID Data Standards Chair's  
15 creditors; or  
16 (iv) makes an assignment of the Digital ID Data Standards  
17 Chair's remuneration for the benefit of the Digital ID  
18 Data Standards Chair's creditors; or  
19 (b) if the Digital ID Data Standards Chair is appointed on a  
20 full-time basis—the Digital ID Data Standards Chair is  
21 absent, except on leave of absence, for 14 consecutive days  
22 or for 28 days in any 12-month period; or  
23 (c) the Digital ID Data Standards Chair fails, without reasonable  
24 excuse, to comply with section 29 of the *Public Governance,  
25 Performance and Accountability Act 2013* (which deals with  
26 the duty to disclose interests) or rules made for the purposes  
27 of that section.

## 28 109 Other terms and conditions

- 29 (1) The Digital ID Data Standards Chair holds office on the terms and  
30 conditions (if any) in relation to matters not covered by this  
31 Division that are determined by the Minister.
- 32 (2) Subsection (1) does not apply while the Digital ID Data Standards  
33 Chair is the Minister.

# EXPOSURE DRAFT

**Chapter 6** Digital ID Data Standards  
**Part 3** Digital ID Data Standards Chair  
**Division 4** Other matters

Section 110

---

1       **Division 4—Other matters**

2       **110 Arrangements relating to staff**

3               (1) The staff assisting the Digital ID Data Standards Chair are to be  
4               APS employees in the Department whose services are made  
5               available to the Chair, by the Secretary, in connection with the  
6               performance of any of the Chair's functions or the exercise of any  
7               of the Chair's powers.

8               (2) When performing services for the Digital ID Data Standards Chair,  
9               the staff are subject to the directions of the Chair.

10       **111 Consultants**

11               (1) The Digital ID Data Standards Chair may, on behalf of the  
12               Commonwealth, engage consultants to assist in the performance of  
13               the Chair's functions or the exercise of the Chair's powers.

14               (2) The consultants are to be engaged on the terms and conditions that  
15               the Digital ID Data Standards Chair determines in writing.

# EXPOSURE DRAFT

Trustmarks and registers **Chapter 7**  
Introduction **Part 1**

Section 112

---

1 **Chapter 7—Trustmarks and registers**

2 **Part 1—Introduction**

3

4 **112 Simplified outline of this Chapter**

# EXPOSURE DRAFT

Chapter 7 Trustmarks and registers

Part 2 Digital ID trustmarks

Section 113

---

## Part 2—Digital ID trustmarks

### 113 Digital ID trustmarks

- (1) The Digital ID Rules may do one or more of the following:
  - (a) specify one or more digital ID trustmarks that may or must be used by accredited entities;
  - (b) specify one or more digital ID trustmarks that may or must be used by participating relying parties;
  - (c) prescribe conditions or requirements in relation to the use or display of those digital ID trustmarks.
- (2) *Digital ID trustmark* means a mark, symbol, logo or design set out in the Digital ID Rules.

### 114 Authorised use of digital ID trustmarks etc.

- (1) An entity is authorised to use a digital ID trustmark if:
  - (a) the Digital ID Rules permit or require the entity to use the digital ID trustmark; and
  - (b) if the Digital ID Rules prescribe conditions in relation to the use or display of the digital ID trustmark—the entity complies with the conditions.
- (2) An entity must not use a digital ID trustmark if the entity is not authorised under subsection (1) to use the trustmark.

Civil penalty:           200 penalty units.
- (3) An entity must not do any of the following in relation to a mark, symbol, logo or design so closely resembling a digital ID trustmark as to be likely to lead a reasonable person to believe that the entity is an accredited entity or a participating relying party:
  - (a) use it in relation to a business, trade, profession or occupation;
  - (b) apply (as a trade mark or otherwise) it to goods imported, manufactured, produced, sold, offered for sale or let on hire;



# EXPOSURE DRAFT

- 1 (c) use it in relation to:  
2 (i) goods or services; or  
3 (ii) the promotion (by any means) of the supply or use of  
4 goods or services.  
5 Civil penalty: 200 penalty units.

## 6 **115 Displaying digital ID trustmark**

- 7 An entity contravenes this subsection if:  
8 (a) the entity is required by the Digital ID Rules to display a  
9 digital ID trustmark in circumstances specified in the Digital  
10 ID Rules; and  
11 (b) the entity fails to comply with the requirement.  
12 Civil penalty: 200 penalty units.

# EXPOSURE DRAFT

Chapter 7 Trustmarks and registers

Part 3 Registers

Section 116

---

## Part 3—Registers

### 116 Digital ID Accredited Entities Register

- (1) The Digital ID Regulator must establish and maintain a register (the *Digital ID Accredited Entities Register*) of entities who are, or have been, accredited entities.
- (2) The Digital ID Accredited Entities Register must contain the following details for each entity:
  - (a) the kinds of accredited entity that the entity is accredited as and the day on which each accreditation came into force;
  - (b) any conditions imposed on the accreditation under subsection 18(2) that are in force, including any variations to those conditions, and the day the condition or variation took effect;
  - (c) any conditions imposed on the accreditation under subsection 18(2) that have been revoked, and the day the revocation took effect;
  - (d) if the entity's accreditation is or has been suspended for a period—that fact and the period of the suspension;
  - (e) if the entity's accreditation is or has been suspended until a specified event occurs or action is taken—that fact and the event or action;
  - (f) if the entity's accreditation is or has been suspended indefinitely—that fact;
  - (g) if the entity's accreditation has been revoked—that fact, and the date the revocation took effect;
  - (h) any other information prescribed by the Digital ID Rules.
- (3) The Digital ID Accredited Entities Register may contain any other information that the Digital ID Regulator considers appropriate.
- (4) If an entity's accreditation is revoked and the entity does not become an accredited entity again for 12 months after the day the revocation came into force, the Digital ID Regulator must remove

- 1 the entity from the Digital ID Accredited Entities Register at the  
2 end of that period.
- 3 (5) The Digital ID Rules may make provision for and in relation to the  
4 following:
- 5 (a) the correction of information in the Digital ID Accredited  
6 Entities register;
- 7 (b) any other matter relating to the administration or operation of  
8 the Digital ID Accredited Entities Register.
- 9 (6) The Digital ID Accredited Entities Register must be made publicly  
10 available on the Digital ID Regulator’s website.
- 11 (7) The Digital ID Accredited Entities Register is not a legislative  
12 instrument.

## 13 **117 AGDIS Register**

- 14 (1) The Digital ID Regulator must establish and maintain a register  
15 (the *AGDIS Register*) of entities who are participating in the  
16 Australian Government Digital ID System.
- 17 (2) The AGDIS Register must contain the following details for each  
18 entity:
- 19 (a) the day the entity’s approval to participate in the Australian  
20 Government Digital ID System came into force;
- 21 (b) the entity’s participation start day;
- 22 (c) if the entity is a participating relying party:
- 23 (i) each service the participating relying party is approved  
24 to provide, or to provide access to, within the Australian  
25 Government Digital ID System;
- 26 (ii) if the participating relying party provides, or may  
27 provide, attributes of individuals obtained from the  
28 Australian Government Digital ID System to other  
29 relying parties—details of those other relying parties,  
30 including the services the other relying parties provide,  
31 or provide access to;

# EXPOSURE DRAFT

## Chapter 7 Trustmarks and registers

### Part 3 Registers

#### Section 117

---

- 1 (d) if the entity is an accredited entity—the kind of accredited  
2 entity it is accredited as;
- 3 (e) any conditions imposed on the entity’s approval to participate  
4 under subsection 62(2) that are in force, including any  
5 variations to those conditions, and the day the condition or  
6 variation took effect;
- 7 (f) any conditions imposed on the entity’s approval to participate  
8 under subsection 62(2) that have been revoked, and the day  
9 the revocation took effect;
- 10 (g) if the entity’s approval to participate is or has been suspended  
11 for a period—that fact and the period of the suspension;
- 12 (h) if the entity’s approval to participate is or has been suspended  
13 until a specified event occurs or action is taken—that fact and  
14 the event or action;
- 15 (i) if the entity’s approval to participate is or has been suspended  
16 indefinitely—that fact;
- 17 (j) if the entity’s approval to participate has been revoked—that  
18 fact, and the date the revocation took effect;
- 19 (k) any other information prescribed by the Digital ID Rules.
- 20 (3) The AGDIS Register may contain any other information that the  
21 Digital ID Regulator considers appropriate.
- 22 (4) If an entity’s approval to participate in the Australian Government  
23 Digital ID System is revoked, and the entity does not hold another  
24 approval to participate in the Australian Government Digital ID  
25 System for 3 years after the day the revocation came into force, the  
26 Digital ID Regulator must remove the entity from the AGDIS  
27 Register at the end of that period.
- 28 (5) The Digital ID Rules may make provision for and in relation to the  
29 following:
- 30 (a) the correction of information in the AGDIS Register;
- 31 (b) any other matter relating to the administration or operation of  
32 the AGDIS Register.
- 33 (6) The AGDIS Register must be made publicly available on the  
34 Digital ID Regulator’s website.

# EXPOSURE DRAFT

Trustmarks and registers **Chapter 7**  
Registers **Part 3**

Section 117

---

- 1 (7) The AGDIS Register is not a legislative instrument.

EXPOSURE DRAFT

# EXPOSURE DRAFT

**Chapter 8** Administration  
**Part 1** Introduction

Section 118

---

1 **Chapter 8—Administration**

2 **Part 1—Introduction**  
3

4 **118 Simplified outline of this Chapter**

1 **Part 2—Compliance and enforcement**

2 **Division 1—Enforcement powers**

3 **119 Civil penalty provisions**

4 *Enforceable civil penalty provisions*

- 5 (1) Each civil penalty provision of this Act is enforceable under Part 4  
6 of the Regulatory Powers Act.

7 Note: Part 4 of the Regulatory Powers Act allows a civil penalty provision to  
8 be enforced by obtaining an order for a person to pay a pecuniary  
9 penalty for the contravention of the provision.

10 *Authorised applicant*

- 11 (2) For the purposes of Part 4 of the Regulatory Powers Act:  
12 (a) the Information Commissioner or a member of staff of the  
13 Office of the Australian Information Commissioner who is an  
14 SES employee or acting SES employee are authorised  
15 applicants in relation to the civil penalty provisions in  
16 Division 2 of Part 2 of Chapter 3 of this Act (about additional  
17 privacy safeguards); and  
18 (b) the Digital ID Regulator is an authorised applicant in relation  
19 to every other civil penalty provision of this Act.

20 *Relevant court*

- 21 (3) For the purposes of Part 4 of the Regulatory Powers Act, each of  
22 the following courts is a relevant court in relation to the civil  
23 penalty provisions of this Act:  
24 (a) the Federal Court of Australia;  
25 (b) the Federal Circuit and Family Court of Australia  
26 (Division 2);  
27 (c) a court of a State or Territory that has jurisdiction in relation  
28 to the matter.

# EXPOSURE DRAFT

Chapter 8 Administration  
Part 2 Compliance and enforcement  
Division 1 Enforcement powers

## Section 120

---

1 **120 Infringement notices**

2 *Provisions subject to an infringement notice*

3 (1) Each civil penalty provision of this Act is subject to an  
4 infringement notice under Part 5 of the Regulatory Powers Act.

5 Note: Part 5 of the Regulatory Powers Act creates a framework for using  
6 infringement notices in relation to provisions.

7 *Infringement officer*

8 (2) For the purposes of Part 5 of the Regulatory Powers Act:

9 (a) the Information Commissioner or a member of staff of the  
10 Office of the Australian Information Commissioner who is an  
11 SES employee or acting SES employee are infringement  
12 officers in relation to the civil penalty provisions in  
13 Division 2 of Part 2 of Chapter 3 of this Act (about additional  
14 privacy safeguards); and

15 (b) the Digital ID Regulator is an infringement officer in relation  
16 to every other civil penalty provision of this Act.

17 *Relevant chief executive*

18 (3) For the purposes of Part 5 of the Regulatory Powers Act, the  
19 relevant chief executive is:

20 (a) in relation to the provisions mentioned in paragraph (2)(a) of  
21 this section—the Information Commissioner; and

22 (b) in relation to the provisions mentioned in paragraph (2)(b) of  
23 this section—the Digital ID Regulator.

24 **121 Enforceable undertakings**

25 *Enforceable provisions*

26 (1) Each civil penalty provision of this Act is enforceable under Part 6  
27 of the Regulatory Powers Act.

28 Note: Part 6 of the Regulatory Powers Act creates a framework for  
29 accepting and enforcing undertakings relating to compliance with  
30 provisions.



# EXPOSURE DRAFT

1 *Authorised person*

- 2 (2) For the purposes of Part 6 of the Regulatory Powers Act:  
3 (a) the Information Commissioner is an authorised person in  
4 relation to the civil penalty provisions in Division 2 of Part 2  
5 of Chapter 3 of this Act (about additional privacy  
6 safeguards); and  
7 (b) the Digital ID Regulator is an authorised person in relation to  
8 every other civil penalty provision of this Act.

9 *Relevant court*

- 10 (3) For the purposes of Part 6 of the Regulatory Powers Act, each of  
11 the following courts is a relevant court in relation to the provisions  
12 mentioned in subsection (1):  
13 (a) the Federal Court of Australia;  
14 (b) the Federal Circuit and Family Court of Australia  
15 (Division 2);  
16 (c) a court of a State or Territory that has jurisdiction in relation  
17 to the matter.

18 *Publishing undertakings*

- 19 (4) The Information Commissioner may publish an undertaking  
20 accepted by the Information Commissioner on the Information  
21 Commissioner's website.  
22 (5) The Digital ID Regulator may publish an undertaking accepted by  
23 the Regulator on the Regulator's website.

24 **122 Injunctions**

25 *Enforceable provisions*

- 26 (1) Each civil penalty provision of this Act is enforceable under Part 7  
27 of the Regulatory Powers Act.

28 Note: Part 7 of the Regulatory Powers Act creates a framework for using  
29 injunctions to enforce provisions.

# EXPOSURE DRAFT

**Chapter 8** Administration  
**Part 2** Compliance and enforcement  
**Division 1** Enforcement powers

## Section 122

---

1

### *Authorised person*

2

(2) For the purposes of Part 7 of the Regulatory Powers Act:

3

(a) the Information Commissioner is an authorised person in relation to the civil penalty provisions in Division 2 of Part 2 of Chapter 3 of this Act (about additional privacy safeguards); and

4

5

6

7

(b) the Digital ID Regulator is an authorised person in relation to every other civil penalty provision of this Act.

8

9

### *Relevant court*

10

(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):

11

12

13

(a) the Federal Court of Australia;

14

(b) the Federal Circuit and Family Court of Australia (Division 2);

15

16

(c) a court of a State or Territory that has jurisdiction in relation to the matter.

17

1 **Division 2—Directions powers**

2 **123 Digital ID Regulator’s power to give directions to entities in**  
3 **relation to participation and accreditation**

- 4 (1) The Digital ID Regulator may give an entity a direction to do a  
5 specified act or thing, or not do a specified act or thing, within the  
6 period specified in the direction if the Digital ID Regulator  
7 considers it necessary to:
- 8 (a) give effect to a decision to approve an entity to participate in  
9 the Australian Government Digital ID System; or
  - 10 (b) give effect to a decision to suspend or revoke an entity’s  
11 approval to participate in the Australian Government Digital  
12 ID System; or
  - 13 (c) to deal with matters arising as a result of the suspension or  
14 revocation of an entity’s approval to participate in the  
15 Australian Government Digital ID System; or
  - 16 (d) give effect to a decision to accredit an entity as an accredited  
17 entity; or
  - 18 (e) give effect to a decision to suspend or revoke an entity’s  
19 accreditation as an accredited entity; or
  - 20 (f) to deal with matters arising as a result of the suspension or  
21 revocation of an entity’s accreditation as an accredited entity.
- 22 (2) Without limiting subsection (1), a direction may:
- 23 (a) require an accredited identity exchange provider to:
    - 24 (i) provide information to an entity that holds an approval  
25 to participate in the Australian Government Digital ID  
26 System about the steps required to connect to the  
27 system; and
    - 28 (ii) connect the entity to the Australian Government Digital  
29 ID System by a specified date; or
  - 30 (b) require an entity whose accreditation has been suspended or  
31 revoked to notify other participants in the digital ID system  
32 in which the entity participates of the suspension or

# EXPOSURE DRAFT

**Chapter 8** Administration  
**Part 2** Compliance and enforcement  
**Division 2** Directions powers

## Section 124

---

- 1 revocation and the date on which the suspension or  
2 revocation takes effect.
- 3 (3) The direction must:  
4 (a) be in writing; and  
5 (b) specify the reason for the direction.
- 6 (4) An entity must comply with a direction given under subsection (1).  
7 Civil penalty: 200 penalty units.
- 8 (5) A direction under subsection (1) is not a legislative instrument.

### **124 Digital ID Regulator's power to give directions to protect the integrity or performance of the Australian Government Digital ID System**

- 9  
10  
11
- 12 (1) The Digital ID Regulator may give a direction to the following  
13 entities if the Digital ID Regulator considers it necessary to do so  
14 to protect the integrity or performance of the Australian  
15 Government Digital ID System:  
16 (a) entities that hold an approval to participate in the Australian  
17 Government Digital ID System;  
18 (b) entities whose approval to participate in the Australian  
19 Government Digital ID System is suspended;  
20 (c) accredited entities;  
21 (d) entities whose accreditation as an accredited entity is  
22 suspended.
- 23 (2) Without limiting subsection (1), the Digital ID Regulator may give  
24 a direction to do one or more of the following:  
25 (a) conduct a privacy impact assessment in relation to a specified  
26 matter and provide a copy of the assessment to the Digital ID  
27 Regulator;  
28 (b) conduct a fraud assessment in relation to a specified matter  
29 and provide a copy of the report to the Digital ID Regulator  
30 in relation to the assessment;

# EXPOSURE DRAFT

## Section 125

---

- 1 (c) conduct a security assessment in relation to a specified matter  
2 and provide a copy of the report to the Digital ID Regulator  
3 in relation to the assessment;  
4 (d) an act or thing specified by the Digital ID Rules.
- 5 (3) If Accreditation Rules made for the purposes of section 27  
6 prescribe requirements in relation to the conduct of an assessment  
7 mentioned in subsection (2), the assessment must comply with the  
8 requirements.
- 9 (4) The direction must:  
10 (a) be in writing; and  
11 (b) specify the reason for the direction.
- 12 (5) An entity must comply with a direction given under subsection (1).  
13 Civil penalty: 200 penalty units.
- 14 (6) A direction under subsection (1) is not a legislative instrument.

### 125 Remedial directions to accredited entities etc.

- 15  
16 (1) This section applies if the Digital ID Regulator reasonably believes  
17 that an accredited entity, or an entity whose accreditation is  
18 suspended, has contravened, or is contravening, a provision of this  
19 Act.
- 20 (2) The Digital ID Regulator may give the entity a direction requiring  
21 the entity to take specified action directed towards ensuring that the  
22 entity does not contravene the provision, or is unlikely to  
23 contravene the provision, in the future.
- 24 (3) The direction must:  
25 (a) be in writing; and  
26 (b) specify the reason for the direction.
- 27 (4) An entity must comply with a direction given under subsection (2).  
28 Civil penalty: 200 penalty units.
- 29 (5) A direction under subsection (2) is not a legislative instrument.

# EXPOSURE DRAFT

Chapter 8 Administration  
Part 2 Compliance and enforcement  
Division 3 Compliance assessments

## Section 126

---

### 1 **Division 3—Compliance assessments**

#### 2 **126 Compliance assessments**

- 3 (1) The Digital ID Regulator may, by written notice, require an entity  
4 to undergo an assessment (a *compliance assessment*):
- 5 (a) for the purposes of determining whether the entity has  
6 complied, is complying or is able to comply with this Act; or
  - 7 (b) if the Digital ID Regulator is satisfied that any of the  
8 following has occurred, or is suspected to have occurred, in  
9 relation to an accredited entity:
    - 10 (i) a cyber security incident;
    - 11 (ii) a digital ID fraud incident;
    - 12 (iii) a serious or repeated breach of the Accreditation Rules;
    - 13 (iv) an incident that is having, or may have, a material  
14 impact on the operation of the entity's information  
15 technology systems through which it provides its  
16 accredited services;
    - 17 (v) an incident that is having, or may have, a material  
18 impact on the operation of the Australian Government  
19 Digital ID System;
    - 20 (vi) a change to the entity's operating environment that is  
21 having, or may have, a material impact on the entity's  
22 risk profile; or
  - 23 (c) in circumstances specified in the Digital ID Rules.

24 Note: For variation and revocation of a notice given under this subsection,  
25 see subsection 33(3) of the *Acts Interpretation Act 1901*.

- 26 (2) The notice must specify:
- 27 (a) the period within which the compliance assessment is to be  
28 undertaken; and
  - 29 (b) whether the compliance assessment must be undertaken:
    - 30 (i) by or on behalf of the Digital ID Regulator; or
    - 31 (ii) by an independent assessor arranged by the entity.

# EXPOSURE DRAFT

## Section 127

---

1 (3) The entity must comply with the notice within the period specified  
2 in the notice.

3 Note 1: If an entity has applied for approval to participate in the Australian  
4 Government Digital ID System and is given a notice under  
5 subsection (1), the Digital ID Regulator is not required to make a  
6 decision on the application until the assessment is conducted (see  
7 subsection 137(4)).

8 Note 2: For accredited entities and entities that hold an approval to participate  
9 in the Australian Government Digital ID System, a failure to comply  
10 with a notice given under subsection (1) may lead to compliance  
11 action such as suspension and revocation of approvals and  
12 accreditation.

13 (4) The Digital ID Rules may make provision for and in relation to  
14 compliance assessments.

15 (5) Without limiting subsection (4), the Digital ID Rules may make  
16 provision for or in relation to the following:

- 17 (a) processes to be followed during a compliance assessment or  
18 after a compliance assessment has been conducted;
- 19 (b) information that must be provided to or by an entity during a  
20 compliance assessment or after a compliance assessment has  
21 been conducted;
- 22 (c) requirements in relation to reports to be provided in relation  
23 to a compliance assessment;
- 24 (d) actions the Digital ID Regulator may require the entity  
25 subject to a compliance assessment to take during the  
26 compliance assessment or after the assessment has been  
27 conducted.

28 (6) This section does not limit the Accreditation Rules that may be  
29 made for the purposes of section 27.

### 30 **127 Entities must provide assistance to persons undertaking** 31 **compliance assessments**

32 An entity that is the subject of a compliance assessment must  
33 provide the person undertaking the assessment with the facilities  
34 and assistance that are reasonably necessary for the conduct of the  
35 compliance assessment.

# EXPOSURE DRAFT

Chapter 8 Administration

Part 2 Compliance and enforcement

Division 4 Power to require information or documents

Section 128

---

1 **Division 4—Power to require information or documents**

2 **128 Power to require information or documents**

3 (1) This section applies if the Digital ID Regulator reasonably believes  
4 that an entity has or may have information or documents relevant  
5 to:

6 (a) whether an entity is complying, or has complied, with the  
7 entity's obligations under this Act; or

8 (b) the performance of the Digital ID Regulator's functions, or  
9 the exercise of any of the Digital ID Regulator's powers,  
10 under this Act.

11 (2) The Digital ID Regulator may, by written notice, require the entity:

12 (a) to give to the Digital ID Regulator, within the period and in  
13 the manner and form specified in the notice, any such  
14 information; or

15 (b) to produce to the Digital ID Regulator, within the period and  
16 in the manner specified in the notice, any such documents.

17 (3) A period specified in a notice under subsection (2) must not be less  
18 than 28 days after the notice is given.

19 (4) A notice under subsection (2) must contain a statement to the effect  
20 that an entity may be liable to a civil penalty if the entity fails to  
21 comply with the notice.

22 (5) An entity must comply with a requirement under subsection (2)  
23 within the period and in the manner specified in the notice.

24 Civil penalty: 200 penalty units.

25 (6) Subsection (5) does not apply if the entity has a reasonable excuse.

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



1 **Part 3—Record keeping**  
2

3 **129 Record keeping by participating entities and former**  
4 **participating entities**

- 5 (1) This section applies to:  
6 (a) entities that hold an approval to participate in the Australian  
7 Government Digital ID System; and  
8 (b) entities whose approval to participate in the Australian  
9 Government Digital ID System is suspended; and  
10 (c) entities whose approval to participate in the Australian  
11 Government Digital ID System has been revoked.

12 (2) However, this section does not apply to relying parties.

13 (3) The entity must keep records of the kind, for the period and in the  
14 manner prescribed by the Digital ID Rules.

15 Civil penalty: 200 penalty units.

- 16 (4) Digital ID Rules made for the purposes of subsection (3):  
17 (a) must not prescribe records of a kind that do not relate to  
18 information obtained by entities through the Australian  
19 Government Digital ID System; and  
20 (b) may only prescribe a period of retention of more than 7 years  
21 if specified circumstances apply in relation to the record.

22 Note: For the purposes of paragraph (b), specified circumstances may  
23 include legal proceedings involving the entity and the records.

24 **130 Destruction or de-identification of certain information**

- 25 (1) This section applies to:  
26 (a) accredited entities that hold an approval to participate in the  
27 Australian Government Digital ID System; and  
28 (b) accredited entities whose approval to participate in the  
29 Australian Government Digital ID System is suspended; and

# EXPOSURE DRAFT

## Chapter 8 Administration

### Part 3 Record keeping

#### Section 130

---

- 1 (c) accredited entities whose approval to participate in the  
2 Australian Government Digital ID System has been revoked.
- 3 (2) The accredited entity must destroy or de-identify information in the  
4 possession or control of the entity if:
- 5 (a) the information is personal information; and  
6 (b) the information was obtained by the entity through the  
7 Australian Government Digital ID System; and  
8 (c) the entity is not required or authorised to retain the  
9 information by or under:
- 10 (i) this Act; or  
11 (ii) another law of the Commonwealth; or  
12 (iii) a law of a State or Territory; or  
13 (iv) a court/tribunal order (within the meaning of the  
14 *Privacy Act 1988*); and  
15 (d) the information does not relate to any current or anticipated  
16 legal proceedings or dispute resolution proceedings to which  
17 the entity is a party.
- 18 Note: For the purposes of subparagraph (c)(i), the entity may be required to  
19 retain the information for a specified period under Digital ID Rules  
20 made for the purposes of section 129.
- 21 Civil penalty: 200 penalty units.

## Part 4—Review of decisions

### 131 Reviewable decisions

- (1) A decision by the Digital ID Regulator referred to in column 1 of an item of the following table is a *reviewable decision*. An entity referred to in column 2 of the item is the *affected entity* for the decision.

<b>Reviewable decisions</b>		
<b>Item</b>	<b>Column 1</b> <i>Reviewable decision</i>	<b>Column 2</b> <i>Affected entity</i>
1	A decision under section 15 to refuse to accredit an entity as an accredited entity	The entity who made the application
2	A decision under subsection 18(2) to impose a condition on an entity's accreditation	The entity on whom the condition is imposed
3	A decision under subsection 18(2) to refuse to impose, on application by an entity, a condition on the entity's accreditation	The entity who made the application
4	A decision under subsection 20(1) to vary, on the Digital ID Regulator's own initiative, the conditions imposed on an entity's accreditation	The entity on whom the conditions are imposed
5	A decision under subsection 20(1) to refuse to vary, on application by an accredited entity, the conditions imposed on the entity's accreditation	The entity who made the application
6	A decision under subsection 25(2) to suspend the accreditation of an accredited entity	The accredited entity
7	A decision under subsection 25(5) to refuse to suspend the accreditation	The accredited entity

# EXPOSURE DRAFT

## Chapter 8 Administration

### Part 4 Review of decisions

#### Section 131

<b>Reviewable decisions</b>		
<b>Item</b>	<b>Column 1</b>	<b>Column 2</b>
	<i>Reviewable decision</i>	<i>Affected entity</i>
	of an accredited entity	
8	A decision under subsection 26(1) to revoke an entity's accreditation	The entity whose accreditation is revoked
9	A decision under section 59 to refuse to approve an entity to participate in the Australian Government Digital ID System	The entity who made the application
10	A decision under subsection 60(2) to direct the Digital ID Regulator to suspend an entity's approval to participate in the Australian Government Digital ID System	The entity subject to the direction
11	A decision under subsection 62(2) to impose a condition on an entity's approval to participate in the Australian Government Digital ID System	The entity on whom the condition is imposed
12	A decision under subsection 62(2) to refuse to impose, on application by an entity, a condition on the entity's approval to participate in the Australian Government Digital ID System	The entity who made the application
13	A decision under subsection 64(1) to vary, on the Digital ID Regulator's own initiative, a condition imposed on an entity's approval to participate in the Australian Government Digital ID System	The entity on whom the condition is imposed
14	A decision under subsection 64(1) to refuse to vary, on application by an entity, a condition imposed on the entity's approval to participate in the Australian Government Digital ID System	The entity who made the application

# EXPOSURE DRAFT

## Section 131

---

### Reviewable decisions

---

<b>Item</b>	<b>Column 1</b> <i>Reviewable decision</i>	<b>Column 2</b> <i>Affected entity</i>
15	A decision under subsection 69(2) to suspend an entity's approval to participate in the Australian Government Digital ID System	The entity that holds the approval
16	A decision under subsection 69(5) to refuse to suspend, on application by an entity, the entity's approval to participate in the Australian Government Digital ID System	The entity who made the application
17	A decision under subsection 69(12) to refuse to revoke a suspension of an entity's approval to participate in the Australian Government Digital ID System	The entity whose approval is suspended
18	A decision under subsection 70(1) to revoke an entity's approval to participate in the Australian Government Digital ID System	The entity that held the approval
19	A decision under subsection 71(3) to refuse to grant an exemption to a participating relying party	The participating relying party who made the application
20	A decision under subsection 81(1) to direct an accredited entity to maintain adequate insurance	The entity subject to the direction
21	A decision to give a direction to an entity under Division 2 of Part 2 of Chapter 8	The entity subject to the direction

---

- 1 (2) The Digital ID Rules may also:
- 2 (a) provide that a decision made under a specified provision of
- 3 this Act is a *reviewable decision*; and
- 4 (b) specify the entity who is an *affected entity* for the reviewable
- 5 decision.

# EXPOSURE DRAFT

## Section 132

---

- 1 (3) If, under subsection (2):  
2 (a) the Digital ID Rules provide that a decision made under the  
3 Digital ID Rules is a reviewable decision; and  
4 (b) the person making the decision is not the Digital ID  
5 Regulator (or a delegate of the Digital ID Regulator);  
6 sections 132, 133 and 134 have effect as if a references in those  
7 sections to the Digital ID Regulator were references to the person  
8 making the decision.
- 9 (4) Despite subsection (1), a decision made for reasons of security  
10 (within the meaning of the *Australian Security Intelligence*  
11 *Organisation Act 1979*) in relation to an entity that is not an  
12 Australian entity is not a *reviewable decision*.

### 132 Internal review of decisions made by delegates of the Digital ID Regulator

- 13  
14
- 15 (1) If an entity is affected by a reviewable decision made by a delegate  
16 of the Digital ID Regulator, the entity may apply in writing to the  
17 Digital ID Regulator for review (the *internal review*) of the  
18 decision.
- 19 (2) An application for internal review must be made within 28 days  
20 after the day on which the decision first came to the notice of the  
21 applicant.

### 133 Reconsideration by Digital ID Regulator

- 22
- 23 (1) Within 90 days after receiving an application under section 132 for  
24 internal review, the Digital ID Regulator must:  
25 (a) review the decision; and  
26 (b) affirm, vary or revoke the decision; and  
27 (c) if the Digital ID Regulator revokes the decision—make such  
28 other decision (if any) that the Digital ID Regulator thinks  
29 appropriate.

# EXPOSURE DRAFT

## Section 134

---

- 1 (2) The Digital ID Regulator must, as soon as practicable after making  
2 a decision under subsection (1), give the applicant a written  
3 statement of the Digital ID Regulator's reasons for the decision.
- 4 (3) If the Digital ID Regulator's functions under this section are  
5 performed by a delegate of the Digital ID Regulator, the delegate  
6 who makes the decision under subsection (1):
- 7 (a) must not have been involved in making the original  
8 reviewable decision; and
- 9 (b) must hold a position or perform duties of a higher level than  
10 the delegate who made the original reviewable decision.

### 11 **134 Review by the Administrative Appeals Tribunal**

- 12 (1) Applications may be made to the Administrative Appeals Tribunal  
13 for review of the following decisions:
- 14 (a) a reviewable decision made by the Digital ID Regulator  
15 personally;
- 16 (b) an internal review decision made by the Digital ID Regulator  
17 under subsection 133(1).
- 18 (2) An application under subsection (1) may be made only by, or on  
19 behalf of, an affected entity for the reviewable decision.
- 20 (3) Subsection (2) has effect despite subsection 27(1) of the  
21 *Administrative Appeals Tribunal Act 1975*.

# EXPOSURE DRAFT

Chapter 8 Administration

Part 5 Applications under this Act

Section 135

---

## Part 5—Applications under this Act

### 135 Requirements for applications

- (1) An application made under this Act must:
- (a) be given in a form and manner for that kind of application approved by the person to whom the application is made; and
  - (b) be accompanied by any information or documents required by the form; and
  - (c) be accompanied by any information or documents required by the Digital ID Rules or the Accreditation Rules; and
  - (d) if Digital ID Rules made for the purposes of section 138 specify a fee that must accompany the application and payment of the fee has not been waived—be accompanied by the fee.

Note: A decision on an application is not required to be made if this subsection is not complied with (see section 137).

- (2) The person to whom the application is made may accept any information or document previously given to the person in connection with another application made under this Act as satisfying any requirement to give that information or document under subsection (1).
- (3) To avoid doubt, approval may be given for:
- (a) different forms for different kinds of applications; or
  - (b) a single form for more than one kind of application.

### 136 Powers in relation to applications

- (1) If a person (the *applicant*) makes an application under this Act, the person to whom the application is made may, by written notice, require the applicant to give the person such further information or documents in relation to the application as the person reasonably requires.



# EXPOSURE DRAFT

## Section 137

---

1 Note 1: The person is not required to make a decision on the application if this  
2 subsection is not complied with (see section 137).

3 Note 2: The Digital ID Regulator may also require an applicant to undergo a  
4 compliance assessment before making a decision on the application  
5 (see section 126).

6 (2) A notice under subsection (1) may specify a period, which must  
7 not be less than 14 days, within which the information or  
8 documents must be given.

### 9 **137 Decisions not required to be made in certain circumstances**

10 (1) If this Act requires an application to be in a form approved by the  
11 person to whom the application is made, the person is not required  
12 to make a decision on the application if it is not in that form.

13 (2) If this Act requires an application to be accompanied by  
14 information or documents, the person to whom the application is  
15 made is not required to make a decision on the application until the  
16 information or documents are provided.

17 (3) If this Act permits a person to require further information or  
18 documents in relation to an application, the person is not required  
19 to make a decision on the application until the information or  
20 documents are provided.

21 (4) If the Digital ID Regulator requires a compliance assessment to be  
22 conducted for the purposes of making a decision under this Act, the  
23 Digital ID Regulator is not required to make the decision until the  
24 assessment is conducted.

25 (5) If Digital ID Rules made for the purposes of section 138 specify a  
26 fee that must accompany an application and payment of the fee has  
27 not been waived, the person to whom the application is made is not  
28 required to make a decision on the application until the fee is paid.

# EXPOSURE DRAFT

Chapter 8 Administration

Part 6 Fees

Division 1 Fees charged by the Digital ID Regulator

Section 138

---

## 1 Part 6—Fees

### 2 Division 1—Fees charged by the Digital ID Regulator

#### 3 138 Charging of fees by Digital ID Regulator etc.

4 (1) The Digital ID Rules may make provision in relation to the  
5 charging of fees by:

6 (a) the Digital ID Regulator for activities carried out by or on  
7 behalf of the Digital ID Regulator in performing functions or  
8 exercising powers under this Act; or

9 (b) other persons to whom application may be made under this  
10 Act.

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

13 (a) prescribe a fee by specifying the amount of the fee or a  
14 method of working out the fee;

15 (b) specify that the amount of a fee is the cost incurred by the  
16 Digital ID Regulator in arranging and paying for another  
17 person to carry out a relevant activity;

18 (c) make provision for when and how fees are to be paid;

19 (d) make provision in relation to penalties for late payment of  
20 specified fees;

21 (e) make provision in relation to the refund, remission or waiver  
22 of specified fees or penalties for late payment of specified  
23 fees.

24 (3) However, the Digital ID Rules made for the purposes of  
25 subsection (1) must not provide for the charging of a fee to an  
26 individual for the creation or use of a digital ID of the individual.

27 (4) A fee prescribed by the Digital ID Rules made under subsection (1)  
28 is payable to the Commonwealth.

29 (5) The amount of a fee may be nil.

# EXPOSURE DRAFT

Administration **Chapter 8**

Fees **Part 6**

Fees charged by the Digital ID Regulator **Division 1**

## Section 139

---

- 1 (6) A fee prescribed by the Digital ID Rules must not be such as to  
2 amount to taxation.
- 3 (7) If a fee is payable for a service, the service need not be provided  
4 while the fee remains unpaid. The Digital ID Rules may provide  
5 for the extension of any times for providing services accordingly.

### 6 **139 Review of fees**

- 7 (1) The Minister must cause periodic reviews of rules made for the  
8 purposes of subsection 138(1) to be undertaken.
- 9 (2) The first review must:  
10 (a) start no later than 2 years after rules made for the purposes of  
11 the relevant subsection commence; and  
12 (b) be completed within 12 months.
- 13 (3) Subsequent reviews must:  
14 (a) start no later than every 2 years after the completion of the  
15 previous review; and  
16 (b) be completed within 12 months.
- 17 (4) The Minister must cause a written report about each review to be  
18 prepared and published on the Digital ID Regulator's website.

### 19 **140 Recovery of fees charged by the Digital ID Regulator**

20 A fee charged by the Digital ID Regulator that is due and payable  
21 to the Commonwealth under this Act may be recovered as a debt  
22 due to the Commonwealth by action in a court of competent  
23 jurisdiction.

### 24 **141 Commonwealth not liable to pay fees charged by entities that** 25 **are part of the Commonwealth**

- 26 (1) The Commonwealth is not liable to pay a fee that is payable under  
27 this Act to a part of the Commonwealth that is not a separate legal  
28 entity. However, it is the Parliament's intention that the  
29 Commonwealth should be notionally liable to pay such a fee.

# EXPOSURE DRAFT

Chapter 8 Administration

Part 6 Fees

Division 1 Fees charged by the Digital ID Regulator

## Section 141

---

- 1 (2) The Finance Minister may give such written directions as are  
2 necessary or convenient for carrying out or giving effect to  
3 subsection (1) and, in particular, may give directions in relation to  
4 the transfer of money within an account, or between accounts,  
5 operated by the Commonwealth.
- 6 (3) Directions under subsection (2) have effect, and must be complied  
7 with, despite any other law of the Commonwealth.
- 8 (4) Directions under subsection (2) are not legislative instruments.
- 9 (5) In this subsection:
- 10 **Commonwealth** includes a Commonwealth entity (within the  
11 meaning of the *Public Governance, Performance and*  
12 *Accountability Act 2013*) that cannot be made liable to taxation by  
13 a law of the Commonwealth.

# EXPOSURE DRAFT

Administration **Chapter 8**

Fees **Part 6**

Fees charged by accredited entities **Division 2**

Section 142

---

1 **Division 2—Fees charged by accredited entities**

2 **142 Charging of fees by accredited entities in relation to the**  
3 **Australian Government Digital ID System**

- 4 (1) An accredited entity that charges fees in relation to its accredited  
5 services that it provides in relation to the Australian Government  
6 Digital ID System must do so in accordance with the Digital ID  
7 Rules (if any) made for the purposes of subsection (2).
- 8 (2) The Digital ID Rules may make provision in relation to the  
9 charging of fees by accredited entities for services provided in  
10 relation to Australian Government Digital ID System.
- 11 (3) Without limiting subsection (2), the Digital ID Rules may do any  
12 of the following:
- 13 (a) prescribe a fee by specifying the amount of the fee or a  
14 method of working out the fee;
- 15 (b) make provision for when and how fees may be charged;
- 16 (c) make provision in relation to the conduct of periodic reviews  
17 of fees;
- 18 (d) make provision for any other matters in relation to the  
19 charging of fees, including in relation to exemptions, refunds,  
20 remissions or waivers.
- 21 (4) The amount of a fee may be nil.
- 22 (5) This section, and rules made for the purposes of subsection (2), do  
23 not otherwise affect the ability of an accredited entity to charge  
24 fees for its accredited services, either in relation to the Australian  
25 Government Digital ID System or otherwise.

## Chapter 9—Other matters

1  
2  
3

### 143 Simplified outline of this Chapter

### 144 Annual report by Digital ID Regulator

6 (1) After the end of each financial year, the Digital ID Regulator must  
7 prepare and give a report to the Minister, for presentation to the  
8 Parliament, on the Digital ID Regulator's activities during the  
9 financial year.

10 (2) The report must include the following:

11 (a) information about the operation of the accreditation scheme,  
12 including:

13 (i) the number of applications for accreditation made under  
14 section 14; and

15 (ii) the number of accreditations granted under section 15;

16 (b) information about the operation of the Australian  
17 Government Digital ID System, including:

18 (i) the number of applications made to participate in the  
19 system under section 58; and

20 (ii) the number of approvals granted to participate in the  
21 system under section 59; and

22 (iii) the number of digital ID fraud incidents or cyber  
23 security incidents, and the responses to any such  
24 incidents;

25 (c) information on any other matters notified by the Minister to  
26 the Digital ID Regulator.

27 (3) The report must be given to the Minister by:

28 (a) the 30th day of October; or

29 (b) the end of any further period granted under  
30 subsection 34C(5) of the *Acts Interpretation Act 1901*.

1 **145 Annual report by Information Commissioner**

2 The annual report prepared by the Information Commissioner and  
3 given to the Minister under section 46 of the *Public Governance,*  
4 *Performance and Accountability Act 2013* for a period must  
5 include information about the performance of the Information  
6 Commissioner's functions, and the exercise of the Information  
7 Commissioner's powers, under or in relation to Part 2 of Chapter 3  
8 of this Act during the period.

9 **146 Treatment of partnerships**

- 10 (1) This Act applies to a partnership as if it were a person, but with the  
11 changes set out in this section.
- 12 (2) An obligation that would otherwise be imposed on the partnership  
13 by this Act is imposed on each partner instead, but may be  
14 discharged by any of the partners.
- 15 (3) A civil penalty provision of this Act that would otherwise have  
16 been contravened by the partnership is taken to have been  
17 contravened by each partner in the partnership, at the time the  
18 provision was contravened, who:
- 19 (a) did the relevant act or made the relevant omission; or  
20 (b) aided, abetted, counselled or procured the relevant act or  
21 omission; or  
22 (c) was in any way knowingly concerned in, or party to, the  
23 relevant act or omission (whether directly or indirectly and  
24 whether by any act or omission of the partner).
- 25 (4) For the purposes of this Act, a change in the composition of a  
26 partnership does not affect the continuity of the partnership.

27 **147 Treatment of unincorporated associations**

- 28 (1) This Act applies to an unincorporated association as if it were a  
29 person, but with the changes set out in this section.
- 30 (2) An obligation that would otherwise be imposed on the association  
31 by this Act is imposed on each member of the association's

# EXPOSURE DRAFT

## Chapter 9 Other matters

### Section 148

---

1 committee of management instead, but may be discharged by any  
2 of the members.

3 (3) A civil penalty provision of this Act that would otherwise have  
4 been contravened by the unincorporated association is taken to  
5 have been contravened by each member of the committee of  
6 management of the association at the time the provision was  
7 contravened, who:

8 (a) did the relevant act or made the relevant omission; or

9 (b) aided, abetted, counselled or procured the relevant act or  
10 omission; or

11 (c) was in any way knowingly concerned in, or party to, the  
12 relevant act or omission (whether directly or indirectly and  
13 whether by any act or omission of the member).

#### 14 **148 Treatment of trusts**

15 (1) This Act applies to a trust as if it were a person, but with the  
16 changes set out in this section.

17 (2) If a trust has a single trustee:

18 (a) an obligation that would otherwise be imposed on the trust by  
19 this Act is imposed on the trustee instead; and

20 (b) a civil penalty provision of this Act that would otherwise  
21 have been contravened by the trust is taken to have been  
22 contravened by the trustee.

23 (3) If a trust has 2 or more trustees:

24 (a) an obligation that would otherwise be imposed on the trust by  
25 this Act is imposed on each trustee instead, but may be  
26 discharged by any of the trustees; and

27 (b) a civil penalty provision of this Act that would otherwise  
28 have been contravened by the relevant entity is taken to have  
29 been contravened by each trustee of the relevant entity, at the  
30 time the provision was contravened, who:

31 (i) did the relevant act or made the relevant omission; or

32 (ii) aided, abetted, counselled or procured the relevant act or  
33 omission; or



- 1 (iii) was in any way knowingly concerned in, or party to, the  
2 relevant act or omission (whether directly or indirectly  
3 and whether by any act or omission of the trustee).

## 4 **149 Treatment of certain Commonwealth, State and Territory** 5 **entities**

### 6 *Government entities*

- 7 (1) This Act applies to any of the following entities (**government**  
8 **entities**) as if it were a person (if it is otherwise not a person), but  
9 with the changes set out in this section:
- 10 (a) a Commonwealth entity (within the meaning of the *Public*  
11 *Governance, Performance and Accountability Act 2013*);
  - 12 (b) a person or body that is an agency within the meaning of the  
13 *Freedom of Information Act 1982*;
  - 14 (c) a body specified, or the person holding an office specified, in  
15 Part I of Schedule 2 to the *Freedom of Information Act 1982*;
  - 16 (d) a department or authority of a State;
  - 17 (e) a department or authority of a Territory.

### 18 *Persons who may engage in conduct on behalf of government* 19 *entities*

- 20 (2) If this Act authorises or requires a government entity to engage in  
21 conduct, the conduct may be engaged in on behalf of the  
22 government entity by a relevant person for the entity, if engaging  
23 in the conduct is within the scope of the relevant person's  
24 employment or authority.

### 25 *Determining how government entities breach this Act*

- 26 (3) In determining whether a government entity has breached this Act:  
27 (a) conduct engaged in on behalf of the entity by a relevant  
28 person for the entity acting within the scope (actual or  
29 apparent) of the relevant person's employment or authority is  
30 taken to have been engaged in instead by the entity; and

# EXPOSURE DRAFT

## Section 149

---

1 (b) if it is necessary to establish intention, knowledge or  
2 recklessness, or any other state of mind, of the entity, it is  
3 sufficient to establish the intention, knowledge or  
4 recklessness, or other state of mind, of the person mentioned  
5 in paragraph (a).

6 (4) Despite paragraph (3)(a), a government entity does not contravene  
7 a civil penalty provision of this Act because of conduct of a person  
8 that the entity is taken to have engaged in, if it is established that  
9 the entity took reasonable precautions and exercised due diligence  
10 to avoid the conduct.

11 *Infringement notices may be given to government entities*

12 (5) If an infringement notice is to be given to the Commonwealth, a  
13 State or a Territory under Part 5 of the Regulatory Powers Act, the  
14 government entity whose acts or omissions are alleged to have  
15 contravened the provision subject to the infringement notice may  
16 be specified in the infringement notice.

17 *Civil penalty proceedings and government entities*

18 (6) If civil penalty proceedings are brought against the  
19 Commonwealth, a State or a Territory in relation to a contravention  
20 of a civil penalty provision of this Act, the government entity  
21 whose acts or omissions are alleged to have contravened the  
22 provision may be specified in any document initiating, or relating  
23 to, the proceedings.

24 (7) Despite paragraph 82(5)(b) of the Regulatory Powers Act, if a  
25 government entity contravenes a civil penalty provision of this Act,  
26 the maximum penalty that a court may order the entity to pay is 5  
27 times the pecuniary penalty specified for the civil penalty  
28 provision.

29 *Relevant person*

30 (8) In this section:

31 ***relevant person*** for an entity means:

- 1 (a) the head (however described) of the entity; or
- 2 (b) a statutory officeholder of the entity; or
- 3 (c) an officer, employee or member of the entity; or
- 4 (d) a person that is party to a contract with the entity; or
- 5 (e) an agent of the entity.

## 6 **150 Bodies corporate and due diligence**

7 For the purposes of section 97 of the Regulatory Powers Act (about  
8 attributing contraventions of employees etc. to a body corporate), a  
9 body corporate does not contravene a civil penalty provision of this  
10 Act because of conduct of a person that the body corporate is taken  
11 to have engaged in, if it is established that the body corporate took  
12 reasonable precautions and exercised due diligence to avoid the  
13 conduct.

## 14 **151 Protection from civil action**

- 15 (1) This section applies to the following:
  - 16 (a) the Digital ID Regulator;
  - 17 (b) a member of the Commission (within the meaning of the
  - 18 *Competition and Consumer Act 2010*);
  - 19 (c) an associate member of the Australian Competition and
  - 20 Consumer Commission;
  - 21 (d) a member of the staff of the Australian Competition and
  - 22 Consumer Commission.
- 23 (2) A person mentioned in subsection (1) is not liable to an action or
- 24 other proceeding for damages for, or in relation to, an act done or
- 25 omitted to be done in good faith by the person:
  - 26 (a) in the performance, or purported performance, of any
  - 27 functions under this Act; or
  - 28 (b) in the exercise, or purported exercise, of any powers under
  - 29 this Act.

## Section 152

---

1 **152 Geographical jurisdiction of civil penalty provisions**

2 *Geographical jurisdiction of civil penalty provisions*

- 3 (1) An entity does not contravene a civil penalty provision of this Act  
4 unless:
- 5 (a) the conduct constituting the alleged contravention occurs  
6 wholly or partly in Australia, or wholly or partly on board an  
7 Australian aircraft or Australian ship; or
  - 8 (b) the conduct constituting the alleged contravention occurs  
9 wholly outside Australia and a result of the conduct occurs:
    - 10 (i) wholly or partly in Australia; or
    - 11 (ii) wholly or partly on board an Australian aircraft or an  
12 Australian ship; or
  - 13 (c) the conduct constituting the alleged contravention occurs  
14 wholly outside Australia and, at the time of the alleged  
15 contravention, the entity is an Australian entity; or
  - 16 (d) all of the following conditions are satisfied:
    - 17 (i) the alleged contravention is an ancillary contravention;
    - 18 (ii) the conduct constituting the alleged contravention  
19 occurs wholly outside Australia;
    - 20 (iii) the conduct constituting the primary contravention to  
21 which the ancillary contravention relates, or a result of  
22 that conduct, occurs wholly or partly in Australia or  
23 wholly or partly on board an Australian aircraft or an  
24 Australian ship.

25 *Defence for primary contravention*

- 26 (2) Despite subsection (1), an entity does not contravene a civil  
27 penalty provision of this Act if:
- 28 (a) the alleged contravention is a primary contravention; and
  - 29 (b) the conduct constituting the alleged contravention occurs  
30 wholly in a foreign country, but not on board an Australian  
31 aircraft or Australian ship; and
  - 32 (c) the entity is not an Australian entity; and

- 1 (d) there is not in force, in the foreign country or the part of the  
2 foreign country where the conduct constituting the alleged  
3 contravention or offence occurred, a law creating a pecuniary  
4 or criminal penalty for conduct corresponding to the conduct  
5 constituting the alleged contravention.

6 *Defence for ancillary contravention*

- 7 (3) Despite subsection (1), an entity does not contravene a civil  
8 penalty provision of this Act if:  
9 (a) the alleged contravention is an ancillary contravention; and  
10 (b) the conduct constituting the alleged contravention occurs  
11 wholly in a foreign country, but not on board an Australian  
12 aircraft or an Australian ship; and  
13 (c) the conduct constituting the primary contravention to which  
14 the alleged contravention relates, or a result of that conduct,  
15 occurs wholly in a foreign country, but not on board an  
16 Australian aircraft or Australian ship; and  
17 (d) the entity is not an Australian entity; and  
18 (e) there is not in force, in the foreign country or the part of the  
19 foreign country where the conduct constituting the alleged  
20 contravention occurred, a law creating a pecuniary or  
21 criminal penalty for conduct corresponding to the conduct  
22 constituting the primary contravention to which the alleged  
23 contravention relates.

24 *Evidential burden*

- 25 (4) An entity who is alleged to have contravened a civil penalty  
26 provision of this Act and who wishes to rely on subsection (2) or  
27 (3) bears an evidential burden (within the meaning of the  
28 Regulatory Powers Act) in relation to the matters set out in the  
29 subsection.

30 *Other matters*

- 31 (5) A reference in this section to a result of conduct is a reference to a  
32 result that is an element of the civil penalty provision.

# EXPOSURE DRAFT

## Chapter 9 Other matters

### Section 153

---

- 1 (6) For the purposes of this section and without limitation, if an entity  
2 sends, or causes to be sent, an electronic communication or other  
3 thing:  
4 (a) from a point outside Australia to a point in Australia; or  
5 (b) from a point in Australia to a point outside Australia;  
6 that conduct is taken to have occurred partly in Australia.

#### 7 *Definitions*

- 8 (7) In this section:

9 ***ancillary contravention*** of a civil penalty provision means a  
10 contravention that arises out of the operation of section 92 of the  
11 Regulatory Powers Act.

12 ***Australian aircraft*** has the same meaning as in the *Criminal Code*.

13 ***Australian ship*** has the same meaning as in the *Criminal Code*.

14 ***electronic communication*** has the same meaning as in the  
15 *Criminal Code*.

16 ***foreign country*** has the same meaning as in the *Criminal Code*.

17 ***point*** includes a mobile or potentially mobile point, whether on  
18 land, underground, in the atmosphere, underwater, at sea or  
19 anywhere else.

20 ***primary contravention*** of a civil penalty provision means a  
21 contravention that does not arise out of the operation of section 92  
22 of the Regulatory Powers Act.

### 23 **153 Review of operation of Act**

- 24 (1) The Minister must cause a review of the operation of this Act to be  
25 undertaken.
- 26 (2) The review must be undertaken no later than 2 years after the  
27 commencement of this Act.

- 1 (3) The persons who undertake the review must give the Minister a  
2 written report of the review.
- 3 (4) The Minister must cause a copy of the report to be tabled in each  
4 House of the Parliament within 15 sitting days of that House after  
5 the Minister receives the report.

## 6 154 Delegation—Minister

- 7 (1) The Minister may, in writing, delegate all or any of the Minister’s  
8 functions or powers under this Act (other than the Minister’s power  
9 under section 158) to any of the following:
- 10 (a) the Digital ID Regulator;  
11 (b) the Secretary;  
12 (c) an SES employee or acting SES employee in the Department.
- 13 Note: Sections 34AA to 34A of the *Acts Interpretation Act 1901* contain  
14 provisions relating to delegations.
- 15 (2) In exercising powers or performing functions under the delegation,  
16 the delegate must comply with any written directions of the  
17 Minister.

## 18 155 Delegation—Digital ID Regulator

- 19 The Digital ID Regulator may, by resolution, delegate all or any of  
20 the Digital ID Regulator’s powers or functions under this Act to:
- 21 (a) member of the Commission (within the meaning of the  
22 *Competition and Consumer Act 2010*); or  
23 (b) an SES employee, or an acting SES employee, in the  
24 Australian Competition and Consumer Commission; or  
25 (c) an SES employee, or an acting SES employee, in the  
26 Department.
- 27 Note 1: The Digital ID Regulator is the Australian Competition and Consumer  
28 Commission (see section 85).
- 29 Note 2: Sections 34AA to 34A of the *Acts Interpretation Act 1901* contain  
30 provisions relating to delegations.

# EXPOSURE DRAFT

## Section 156

---

1 **156 Delegation—Digital ID Data Standards Chair**

- 2 (1) The Digital ID Data Standards Chair may delegate, in writing, any  
3 or all of the Chair’s functions or powers to a person assisting the  
4 Chair under section 110 who is:  
5 (a) an SES employee, or an acting SES employee; or  
6 (b) an APS employee who is holding or performing the duties of  
7 a specified office or position that the Chair is satisfied is  
8 sufficiently senior for the APS employee to perform the  
9 function or exercise the power.
- 10 (2) Subsection (1) does not apply to the function referred to in  
11 paragraph 93 (about making standards).
- 12 (3) In performing a delegated function or exercising a delegated  
13 power, the delegate under subsection (1) must comply with any  
14 directions of the Digital ID Data Standards Chair.

15 **157 Instruments may incorporate etc. material as in force or existing**  
16 **from time to time**

- 17 (1) This section applies to the following instruments (each of which is  
18 a *core instrument*):  
19 (a) the Accreditation Rules;  
20 (b) the Digital ID Data Standards;  
21 (c) the Digital ID Rules.
- 22 (2) A core instrument may make provision in relation to a matter by  
23 applying, adopting or incorporating, with or without modification,  
24 any matter contained in any other instrument or other writing (an  
25 *incorporated instrument*) as in force or existing from time to time.
- 26 (3) If a core instrument makes provision in relation to a matter in  
27 accordance with subsection (2), the core instrument may also make  
28 provision in relation to when changes to an incorporated  
29 instrument take effect for the purposes of the core instrument.
- 30 (4) Subsection (2) has effect despite subsection 14(2) of the  
31 *Legislation Act 2003*.



1 **158 Rules—general matters**

- 2 (1) The Minister may, by legislative instrument, make rules  
3 prescribing matters:  
4 (a) required or permitted by this Act to be prescribed by the  
5 rules; or  
6 (b) necessary or convenient to be prescribed for carrying out or  
7 giving effect to this Act.
- 8 (2) Without limiting subsection 33(3A) of the *Acts Interpretation Act*  
9 *1901*, the rules may prescribe a matter or thing differently for  
10 different kinds of entities, things or circumstances.
- 11 (3) The rules may make provision for or in relation to a matter by  
12 conferring a power on the Digital ID Regulator or the Minister to:  
13 (a) make an instrument of an administrative character; or  
14 (b) make a decision of an administrative character.
- 15 (4) To avoid doubt, the rules may not do the following:  
16 (a) create an offence or civil penalty;  
17 (b) provide powers of:  
18 (i) arrest or detention; or  
19 (ii) entry, search or seizure;  
20 (c) impose a tax;  
21 (d) set an amount to be appropriated from the Consolidated  
22 Revenue Fund under an appropriation in this Act;  
23 (e) directly amend the text of this Act.
- 24 (5) In this section, a reference to this Act does not include a reference  
25 to:  
26 (a) the Accreditation Rules; or  
27 (b) the Digital ID Rules.

# EXPOSURE DRAFT

## Section 159

---

1 **159 Rules—requirement to consult**

2 *General requirement to consult*

- 3 (1) Before making or amending any rules under section 158, the  
4 Minister must:
- 5 (a) cause to be published on the Department’s website a notice:  
6 (i) setting out the draft rules or amendments; and  
7 (ii) inviting persons to make submissions to the Minister  
8 about the draft rules or amendments within the period  
9 specified in the notice (which must be at least 28 days  
10 after the notice is published); and  
11 (b) if the rules deal with matters that relate to the privacy  
12 functions (within the meaning of the *Australian Information*  
13 *Commissioner Act 2010*)—consult the Information  
14 Commissioner; and  
15 (c) consider any submissions received within the specified  
16 period.
- 17 (2) Without paragraph (1)(b), the Minister must consult the  
18 Information Commissioner if the rules will provide that accredited  
19 entities, or specified kinds of accredited entities, are authorised to:  
20 (a) collect or disclose restricted attributes of individuals; or  
21 (b) collect, use or disclose biometric information of individuals.
- 22 (3) The Minister may consider any submissions received after the  
23 specified period if the Minister considers it appropriate to do so.

24 *Exception if imminent threat etc.*

- 25 (4) Subsection (1) does not apply if:  
26 (a) the Minister is satisfied that there is an imminent threat to the  
27 Australian Government Digital ID System; or  
28 (b) the Minister is satisfied that a hazard has had, or is having, a  
29 significant impact on the Australian Government Digital ID  
30 System.

1

*Review*

2

(5) If:

3

(a) because of subsection (4), subsection (1) did not apply to the making of rules or amendments; and

4

5

(b) the rules or amendments have not been disallowed by either House of the Parliament;

6

7

the Secretary must:

8

(c) review the operation, effectiveness and implications of the rules or amendments; and

9

10

(d) without limiting paragraph (a), consider whether any amendments should be made; and

11

12

(e) give the Minister a report of the review and a statement setting out the Secretary's findings.

13

14

(6) For the purposes of the review, the Secretary must:

15

(a) cause to be published on the Department's website a notice:

16

(i) setting out the rules or amendments concerned; and

17

(ii) inviting persons to make submissions to the Secretary

18

about the rules or amendments concerned within the

19

period specified in the notice (which must be at least 28

20

days after the notice is published); and

21

(b) if the rules deal with matters that relate to the privacy

22

functions (within the meaning of the *Australian Information*

23

*Commissioner Act 2010*)—consult the Information

24

Commissioner; and

25

(c) consider any submissions received within the specified

26

period.

27

*Findings of review to be tabled*

28

(7) The Secretary must complete the review within 60 days after the commencement of the rules or amendments concerned.

29

30

(8) The Minister must cause a copy of the statement of findings to be

31

tabled in each House of the Parliament within 15 sitting days of

32

that House after the Minister receives it.

# EXPOSURE DRAFT

## Chapter 9 Other matters

### Section 159

---

1 *Failure to comply does not affect validity etc.*

2 (9) A failure to comply with this section does not affect the validity or  
3 enforceability of any rules, or any amendments to any rules.

4 *Relationship with the Legislation Act 2003*

5 (10) This section does not limit section 17 of the *Legislation Act 2003*  
6 (rule-makers should consult before making legislative instrument).