Electronic Identity Verification Bill

Government Bill

Explanatory note

General policy statement

The purpose of this Bill is to regulate the administration and application of the Electronic Identity Verification Service. The service is designed to provide individuals with the option of a quick, easy, and secure way to verify their identity via the Internet (ie, to a standard comparable with presenting a passport at a counter). It will allow individuals to access a range of services from authorised agencies, where it is necessary for those agencies to have a degree of confidence in individuals' identity.

If an individual chooses to apply to use the Electronic Identity Verification Service, an electronic record of a small amount of personal information will be created and held by the service, which is operated by the Department of Internal Affairs. The individual will be able to authorise the release of the stored identity information to an authorised agency. His or her identity will then be verified using an identifier or code, derived from the stored electronic record, that is unique to the authorised agency. This approach is designed to prevent unauthorised use and sharing of the information by agencies. This process could occur via a computer at an agency's counter, for face-to-face transactions.

The service is designed to allow people to avoid the cost and inconvenience of repeatedly having to prove their identity in person to dif-

ferent agencies, and avoids the need for those agencies to invest in their own online identity verification infrastructure and capability. The service will provide a secure and consistent way for agencies to verify the identity of a person interacting with it while being user-focused and protective of individuals' privacy. An individual's use of the service is optional. Other ways of interacting with agencies remain available.

The Bill outlines the purposes and boundaries of the Electronic Identity Verification Service. It specifies that anyone may apply to use the service (except where prevented by court order), with parental or guardian's consent being required for those under 14 years old. Agencies authorised to verify individuals' identity information through the service will be listed in regulations, allowing the service to be used for the widest range of services possible. The Bill would allow both public and private sector agencies to be listed.

To help ensure the integrity of the service, the Bill allows individuals' personal information to be checked against information held on specified government registers and databases, subject to the usual controls applying to authorised information matching programmes. The Bill also allows personal information to be checked, with the consent of the individual, against information held by public sector or private sector agencies that are listed in regulations for that purpose, and in accordance with the terms of agreements between the Department of Internal Affairs and those agencies. In those latter cases, agencies would confirm whether or not the personal information is consistent with the information held on their records, but would not disclose additional personal information.

The Bill strictly regulates access to personal information held on the Electronic Identity Verification Service's computer systems. The Privacy Commissioner will be able to require the chief executive of the Department of Internal Affairs to report on the general operation of the service from time to time, as well as monitoring the information matching programmes, and dealing with any complaints about privacy breaches associated with the service.

The service's features, as set out in the Bill, also help to protect people's privacy interests in their personal information. The service does not involve the issuing of a physical card with a universal unique identifier to members of the public. The Bill prescribes a minimal range of information that can be collected, held, and used. People

will be provided with their personal information to check before it is sent to an agency and they will have control over whether or not it is sent. As an individual's identity is proven to a high level of confidence when the individual applies to use the service, and because of the secure way an individual's information is used, the risks of other people impersonating that individual are reduced.

Specific offences and penalties are created to deter abuse of the service, while existing offences apply to the fraudulent use of a person's identity information in the same way as they would for the presentation of paper-based forms of identification. The Bill allows the costs of running the service to be recovered through fees, either as prescribed by regulations or as set by contract.

From December 2009, the Department of Internal Affairs has operated the Identity Verification Service (as the "igovt identity verification service") on a limited, contractual, basis. The service will be expanded, through the Bill's provisions, to be made available to the general public and will involve a wider range of organisations. To ensure a smooth and co-ordinated transition from the existing arrangements, it is proposed that the substantive provisions of the Bill would be brought into force by way of Order in Council or, at the very latest, 12 months after the date on which the Bill receives the Royal assent.

Regulating the administration of the Electronic Identity Verification Service through legislation means that its boundaries (including its opt-in nature) will not arbitrarily be changed, and ensures there is clear authority for controls to be exercised to protect the service from abuse.

Regulatory impact assessment

The Department of Internal Affairs produced a regulatory impact statement on 8 February 2011 to help inform the main policy decisions taken by the Government in this Bill.

A copy of this regulatory impact statement can be found at—

- http://www.dia.govt.nz/Resource-material-Regulatory-Impact-Statements-Index#one
- http://www.treasury.govt.nz/publications/informationreleases/ris

Clause by clause analysis

Clause 1 is the Title clause.

Clause 2 is the commencement clause. *Parts 2 and 3* (except *clauses 63 to 67*) and *Schedules 1 and 2* will come into force on a date appointed by the Governor-General by Order in Council. Any provisions of *Parts 2 and 3 and Schedules 1 and 2* that have not been brought into force on the day that is 12 months after the date on which the Bill receives the Royal assent will come into force on that day. The rest of the Bill will come into force on the day after the date on which it receives the Royal assent.

Part 1
Preliminary provisions

Clause 3 states the purpose of the Bill, which is to facilitate secure interactions (particularly online interactions) between individuals on the one hand and participating agencies on the other by enabling individuals' identities to be verified by electronic means.

Clause 4 sets out principles on which the Bill is based. The principles do not confer on any person any legal right that is enforceable, for example, in a court of law.

Clause 5 provides an overview of the Bill's provisions.

Clause 6 states that the Bill binds the Crown.

Clause 7 contains definitions of some terms used in the Bill.

Part 2
Electronic identity verification

Subpart 1—Electronic identity credential

Clause 8 defines an electronic identity credential.

Clause 9 specifies the contents of an electronic identity credential.

Clause 10 provides that an electronic identity credential is effective for the period prescribed in regulations made under the Act, unless it is sooner cancelled or revoked.

Clause 11 provides that, subject to *clause 12*, there must be no more than 1 electronic identity credential for each individual at any given time.

Clause 12 sets out an exception to the requirement in *clause 11*. The exception applies to certain specified individuals for whom new identity information has been created under section 65 of the Births, Deaths, Marriages, and Relationships Registration Act 1995 (which relates to the protection of certain witnesses, undercover police officers, and other protected persons). The specified individuals are undercover police officers, officers or employees of the New Zealand Security Intelligence Service, and persons approved by the Director of Security to undertake activities for the New Zealand Security Intelligence Service. Under *clause 12*, a specified individual may apply for, and use, an electronic identity credential in respect of his or her original identity, or his or her new identity, or both identities.

Clause 13 sets out limits to the exception in *clause 12*. It provides that the exception does not apply to 2 of the other categories of individuals for whom new identity information may be created under section 65 of the Births, Deaths, Marriages, and Relationships Registration Act 1995. Those categories are witnesses in proceedings who are not specified individuals, and individuals who may need protection because of their relationships to persons who are, have been, or will be witnesses in proceedings. These 2 categories of individuals will continue to be subject to the requirement in *clause 11* and they can only have 1 electronic identity credential issued to each of them at any time. Accordingly, if they already have an electronic identity credential at the time the new identity information is created, the chief executive of the Department of Internal Affairs must cancel that original electronic identity credential in accordance with *clause 29* and may, on application, issue a new credential in respect of the individual's new identity.

Clause 14 provides that an electronic identity credential is personal to the individual to whom it has been issued and may not be transferred or vest by operation of law in any other person.

Clause 15 provides that an individual does not have any property rights in an electronic identity credential that has been issued to him or her.

Clause 16 sets out restrictions on the use of an electronic identity credential.

Clause 17 describes the uses to which an electronic identity credential may be put by an individual.

Clause 18 provides that a participating agency may use core identity information contained in an individual's electronic identity credential, information derived from, or based on, that core identity information, or associated information to verify an individual's identity by electronic means. A participating agency may, among other things, choose the types of transactions or services offered by it that are to be transactions or services for which the identity of an individual may be verified by electronic means.

Clause 19 describes the legal effect of using an electronic identity credential. It provides that a legal requirement to supply information about an individual's identity to a participating agency is met by the individual giving consent to the Service to supply all or any of the core identity information contained in the individual's current electronic identity credential to the agency. It also provides that a legal requirement to provide a signature to a participating agency is met by the individual giving consent to the Service to supply the individual's current electronic identity credential to the agency.

Clause 20 provides that the expiry, amendment, cancellation, suspension, or revocation of an electronic identity credential does not affect the validity of any transaction or service that was completed or provided before the change even if the identity of the individual to whom the transaction or service relates was verified using that credential.

Clause 21 specifies who may access the record of usage history of an electronic identity credential.

Clauses 22 to 27 contain requirements for applications for electronic identity credentials, including provisions about what kinds of applications may be made and who may make them.

Clause 28 requires the chief executive to amend an electronic identity credential in certain circumstances.

Clause 29 requires the chief executive to cancel an electronic identity credential in certain circumstances.

Clause 30 allows the chief executive to suspend the processing of an application for an electronic identity credential or an individual's electronic identity credential if—

- the individual is under investigation for an offence against the Bill, an offence against any other enactment involving the use of an electronic identity credential, or an offence against any

other enactment involving a computer system on which the operation of the Service database relies; or

- the chief executive has reasonable grounds to believe that the individual is liable to prosecution or is the subject of a charge in respect of such an offence.

Clause 31 allows the chief executive to revoke an individual's electronic identity credential if the chief executive is satisfied, after proper inquiries, that the credential was issued, renewed, or amended on the basis of any false or fraudulent representation or declaration, or was issued or renewed in error.

Clause 32 sets out the process that the chief executive must follow before exercising the power of suspension conferred by *clause 30* or the power of revocation conferred by *clause 31*.

Subpart 2—Administrative provisions

Clauses 33 to 36 contain provisions dealing with the disclosure of identity-related information to the chief executive and the Service for the purpose of helping the chief executive to authenticate an individual's identity and to keep the core identity information contained in an individual's electronic identity credential accurate and up to date.

Clauses 37 to 47 set out the functions, duties, and powers of the chief executive, which include—

- the duty to take all reasonable steps to authenticate an individual's identity (including by means of the information-matching process provided for by *clauses 33 to 36* or the mechanism for identity information checks set out in *Schedule 1*); and
- the power to set standards or specifications for the use of electronic identity credentials by participating agencies; and
- the power to suspend the use of electronic identity credentials by participating agencies; and
- the power to enter into an agreement with a third party for the performance of functions and duties, or the exercise of powers, under the Act.

Clause 48 provides that the Ombudsmen Act 1975 and the Official Information Act 1982 apply to the chief executive's delegate who is not

an employee of the State services and to a third party that performs the chief executive's functions and duties, or exercises the chief executive's powers, under the Bill in accordance with an agreement entered into under *clause 47(1)(b)*.

Clauses 49 and 50 provide for the reconsideration of decisions made by the chief executive under the Act.

Clause 51 describes the Electronic Identity Verification Service.

Clause 52 sets out the function of the Service.

Clause 53 enables the Privacy Commissioner to require the chief executive to prepare a report on the operation of the Electronic Identity Verification Service or on the operation of confirmation agreements under *Schedule 1*, or on both.

Part 3
Miscellaneous provisions

Clause 54 explains the relationship between the Bill and the Official Information Act 1982.

Clause 55 explains the relationship between the Bill and the Privacy Act 1993.

Clauses 56 to 59 set out offences against the Bill and the penalties for those offences.

Clause 60 empowers a court, when sentencing an individual for a specified offence, to make all or any of the following orders:

- an order that an electronic identity credential must not be issued to the individual, either indefinitely or for any period that may be specified in the order:
- an order that an electronic identity credential that has been issued to the individual be revoked:
- an order giving any direction that the court thinks fit about the validity of any applicable transaction or service that was completed or provided as a result of, or in connection with, the commission of the specified offence.

A specified offence in this context is defined in *clause 7* to mean an offence against the Bill, an offence against any other enactment involving the use of an electronic identity credential, or an offence against any other enactment involving a computer system on which the operation of the Service database relies.

Clause 61 protects the chief executive and any employee or agent of the department from criminal or civil liability in respect of any act done or omitted in the course of the exercise or performance or intended exercise or performance of their functions, duties, or powers under the Act. It also protects the Crown, Ministers of the Crown, and other persons from any liability for damages for any loss or damage that is due directly or indirectly to the use of an electronic identity credential to verify an individual's identity.

Clause 62 contains requirements about the giving of notices or any other document under the Act or any regulation made under the Act.

Clauses 63 to 67 provide for regulations to be made under the Act.

Clauses 68 and 69 are transitional provisions relating to electronic identity credentials that were issued before the commencement of the Act.

Clause 70 is also a transitional provision relating to an agreement that was entered into before the commencement of the Act between the chief executive and a third party for the third party to perform the chief executive's functions and duties, or to exercise the chief executive's powers, under the Bill. *Clause 70* clarifies that the agreement is to be treated as if it were an agreement entered into under *clause 47(1)(b)* (except that *clause 47(2)* does not apply).

Clause 71 provides for consequential amendments to be made to other enactments.

Schedule 1 sets out a mechanism that allows the chief executive to authenticate an individual's identity for the purposes of the Bill by providing for identity information checks. It is based on the model set out in the Identity Information Confirmation Bill (which is currently before the House of Representatives), but provides for identity information to be checked against information held by various agencies rather than against information held by the Department of Internal Affairs under the Births, Deaths, Marriages, and Relationships Registration Act 1995, the Citizenship Act 1977, and the Passports Act 1992.

Schedule 2 sets out consequential amendments to other enactments.

Hon Nathan Guy

Electronic Identity Verification Bill

Government Bill

Contents

The Parliament of New Zealand enacts as follows:

1 Title

This Act is the Electronic Identity Verification Act **2011**.

2 Commencement

(1) **Parts 2 and 3** (except **sections 63 to 67**) and **Schedules 1 and 2** come into force on a date appointed by the Governor-General by Order in Council and 1 or more Orders in Council may be made appointing different dates for different provisions and for different purposes.

(2) Any provisions of **Parts 2 and 3 and Schedules 1 and 2** that are not in force on the day that is 12 months after the date on which this Act receives the Royal assent come into force on that day.

(3) The rest of this Act comes into force on the day after the date on which it receives the Royal assent.

Part 1
Preliminary provisions

3 Purpose

(1) The purpose of this Act is to facilitate secure interactions (particularly online interactions) between individuals on the one hand and participating agencies on the other.

(2) To that end, this Act—

(a) ensures that participating agencies can achieve a high degree of confidence in an individual's identity by providing the individual with the option of verifying his or her identity authoritatively and in real time by electronic means if a degree of confidence is necessary for the interaction between the participating agency and the individual; and

(b) provides for a whole of government shared service to enable a centralised approach to be taken in relation to the verification of an individual's identity by electronic means while protecting the individual's privacy.

4 Principles

(1) This Act is based on the following principles:

(a) an individual has a complete discretion to decide whether to apply for an electronic identity credential to be issued to him or her and whether to use it at all if it has been issued:

(b) an individual may continue to access the services of a participating agency by means other than by using an electronic identity credential even though an electronic identity credential has already been issued to him or her:

(c) the use of an electronic identity credential does not, of itself, limit or affect the need for an individual, if required,—

(i) to show that he or she is qualified or eligible for a particular service offered by a participating agency; and

(ii) to authorise the agency to act on a particular matter or transaction:

(d) an individual's consent to the supply of his or her personal information to a participating agency must be obtained before the Service can supply the information to the agency and, even if the consent is obtained, the Service may supply only the minimum amount of personal information that is necessary for the agency to act as part of a given transaction or a series of transactions:

(e) an individual may check whether information held about him or her by the Service is correct and up to date:

(f) an individual has the right to view the usage history of his or her electronic identity credential.

(2) The chief executive, the Service, every employee or contractor of the department, and every participating agency must, in making decisions, performing functions or duties, or exercising powers under this Act, take into account those principles specified in **subsection (1)** that are applicable (if any), so far as is practicable in the circumstances.

(3) **Subsections (1) and (2)** do not—

(a) override any other provision in this Act or any other enactment; and

(b) confer on any person any legal right that is enforceable, for example, in a court of law.

5 Overview

(1) **Part 1** deals with preliminary matters, including the purpose of this Act, the principles on which this Act is based, the application of this Act to the Crown, and interpretation.

(2) **Part 2** deals with matters relating to electronic identity verification, including—

- (a) provisions that set out requirements governing the use of electronic identity credentials for the purpose of verifying an individual's identity:
- (b) provisions relating to administrative matters that underpin the substantive provisions dealing with electronic identity verification (for example, the disclosure of identity-related information to the chief executive and the Service, the functions, duties, and powers of the chief executive, the reconsideration of decisions made by the chief executive under this Act, and the function of the Service).

(3) **Part 3** deals with miscellaneous matters, including—

- (a) the application of other Acts:
- (b) offences and penalties:
- (c) court orders relating to specified offences:
- (d) protection of the Crown and other persons from liability:
- (e) requirements for notices given under this Act:
- (f) regulation-making powers:
- (g) transitional provisions:
- (h) consequential amendments to other enactments.

(4) **Schedule 1** sets out a mechanism that allows the chief executive to authenticate an individual's identity for the purposes of this Act. It provides for identity information checks to be carried out by agencies (whether in the public sector or private sector) under confirmation agreements with the chief executive.

(5) **Schedule 2** sets out consequential amendments to other enactments.

(6) This section is only a guide to the general scheme and effect of this Act.

6 Act binds the Crown

This Act binds the Crown.

7 Interpretation

In this Act, unless the context otherwise requires,—

applicable transaction or service means a transaction or service chosen by a participating agency under **section 18(3)(a)** as a transaction or service for which the identity of an individual may be verified by electronic means

applicant, except in **section 50**, means—

(a) an individual who makes or has made, as the case may be, an application; and

(b) a child under 14 years of age on whose behalf an application is, or has been, made, as the case may be

application, except in **sections 19(2)(a) and 50**, means any of the applications referred to in **section 22**, as the case may be

associated information—

(a) means technical information consisting of a randomly generated code for each electronic identity credential that—

  (i) is unique to a participating agency; and

  (ii) is additional to, and a derivative of, the unique code referred to in **section 8**; and

(b) includes information about the status of the electronic identity credential; but

(c) does not include the usage history of the electronic identity credential or any information from which the usage history could be derived

authenticated means the state of having been confirmed, to the reasonable satisfaction of the chief executive, as being authoritative

cancellation, in relation to an electronic identity credential, means, as the case may be,—

(a) voluntary cancellation under **section 27**; and

(b) mandatory cancellation under **section 29**

chief executive means the chief executive of the department

conviction on indictment has the same meaning as convicted on indictment in section 3 of the Crimes Act 1961

core identity information means the information specified in **section 9(1)**

current, in relation to an electronic identity credential, means that the electronic identity credential has been issued and has not expired or is not cancelled, suspended, or revoked

department means the department of State that is, with the authority of the Prime Minister, for the time being responsible for the administration of this Act

electronic includes electrical, digital, magnetic, optical, electromagnetic, and photonic

electronic identity credential has the meaning given to it by **section 8**

electronic signature, in relation to information in electronic form, means a method used to identify an individual and to indicate that individual's approval of that information

identity-related information—

(a) means any or all of the following:

(i) adoption information, birth information, death information, marriage information, civil union information, and name change information under the Births, Deaths, Marriages, and Relationships Registration Act 1995:

(ii) citizenship information (within the meaning of section 26A(6) of the Citizenship Act 1977):

(iii) identifying information (within the meaning of section 303(8) of the Immigration Act 2009, except that it also includes the expiry date of any visa granted to the individual (if applicable)):

(iv) New Zealand travel document information of a kind referred to in section 37 of the Passports Act 1992:

(b) includes a photograph of the individual to whom the information referred to in **paragraph (a)** relates

individual means a natural person, except a deceased natural person

law enforcement agency means—

(a) the New Zealand Police; or

(b) any government department declared by the Governor-General, by regulations made under **section 67(a)**, to be a law enforcement agency for the purposes of this Act

Minister means the Minister of the Crown who is, with the authority of the Prime Minister, for the time being responsible for the administration of this Act

participating agency means a person, body, or office declared by the Governor-General, by regulations made under **section 63**, to be a participating agency for the purposes of this Act

photograph includes any electronic record of the photograph

pre-commencement electronic identity credential has the meaning given to it by **section 68**

Privacy Commissioner means the Privacy Commissioner appointed under section 12 of the Privacy Act 1993

record of usage history means the record that the chief executive is required to keep under **section 40** about the usage history of each electronic identity credential

Registrar-General has the meaning given to it by section 2 of the Births, Deaths, Marriages, and Relationships Registration Act 1995

Service means the Electronic Identity Verification Service described in **section 51**

Service database means an electronic file, register, or device in or on which information is or is to be recorded or stored by the Service or employees of the department for the purposes of this Act

specified individual has the meaning given to it by **section 12(2)**

specified offence means any of the following, as the case may be:

(a) an offence against this Act:

(b) an offence against any other enactment involving the use of an electronic identity credential:

(c) an offence against any other enactment involving a computer system on which the operation of the Service database relies

State services has the meaning given to it by section 2 of the State Sector Act 1988

status, in relation to an electronic identity credential, means the currency, expiry, amendment, cancellation, suspension, or revocation of the electronic identity credential

usage history means information about each occasion that—

(a) an individual uses the individual's electronic identity credential:

(b) a participating agency uses an individual's electronic identity credential:

(c) any of the persons referred to in **section 21(1)** accesses the information referred to in **paragraph (a) or (b)**

use,—

(a) in relation to the use of an electronic identity credential by an individual, means to use the credential for any of the uses described in **section 17(2)**; or

(b) in relation to the use of an electronic identity credential by a participating agency, means to use the credential to verify the identity of an individual by electronic means.

Part 2
Electronic identity verification

Subpart 1—Electronic identity credential

General

8 Electronic identity credential: definition

An **electronic identity credential** is a record kept in electronic form that—

(a) contains authenticated core identity information about an individual; and

(b) is assigned a unique code by the Service.

9 Electronic identity credential: contents

(1) An electronic identity credential may contain as much of the following core identity information about an individual as it is possible to authenticate:

(a) the individual's full name:

(b) the individual's sex:

(c) the individual's date of birth:

(d) the individual's place of birth.

(2) The following table sets out details relating to core identity information that may also be included in an electronic identity credential:

Core identity information	Details that may be included
Full name	May include all or any of the following: (a) the individual's current name (that is, the individual's name at the time of applying for an electronic identity credential to be issued): (b) the individual's full name at birth (if different from the current name): (c) other names the individual has used before applying for an electronic identity credential to be issued or renewed: (d) other names the individual may use while an electronic identity credential is current (for example, a name change registered under section 21B of the Births, Deaths, Marriages, and Relationships Registration Act 1995 or under a corresponding provision in overseas legislation)
Sex	May include all or any of the following: (a) the individual's sex as recorded at birth: (b) the individual's nominated sex if the individual can provide to the chief executive evidence of a sex change (for example, a declaration of the Family Court under section 28 or 29 of the Births, Deaths, Marriages, and Relationships Registration Act 1995)

Core identity information	Details that may be included
Date of birth	May include day, month, and year of birth
Place of birth	May include all or any of the following details about the individual's place of birth: (a) locality or town or city: (b) state or province or territory: (c) country

(3) **Subsection (1)** is subject to **section 24(2)(b)** and the absence of 1 or more items of core identity information about an individual does not, therefore, prevent an electronic identity credential from being issued to the individual if the chief executive otherwise considers that the identity of the individual has been authenticated.

10 Electronic identity credential: duration

(1) An electronic identity credential is effective for the period prescribed in regulations made under **section 67**.

(2) **Subsection (1)** applies unless the electronic identity credential—

(a) is cancelled by the chief executive under **section 27 or 29**; or

(b) is revoked by the chief executive under **section 31**; or

(c) is revoked by order of a court under **section 60(1)(b)**.

(3) An electronic identity credential may be renewed, in accordance with **section 25**, for a further period or periods prescribed in regulations.

11 Only 1 electronic identity credential per individual

(1) There must be no more than 1 electronic identity credential for each individual at any given time.

(2) This section is subject to **section 12**.

12 Exception to section 11 for certain individuals with new identity information

(1) **Section 11** does not apply to an individual who is specified in **subsection (2)** for whom new identity information has been created under section 65 of the Births, Deaths, Marriages, and

Relationships Registration Act 1995 (which relates to the protection of certain witnesses, undercover police officers, and other protected persons).

(2) An individual referred to in **subsection (1)** (a **specified individual**) is a person who is, has been, or will be—
- (a) an undercover police officer; or
- (b) an officer or employee of the New Zealand Security Intelligence Service; or
- (c) approved by the Director of Security to undertake activities for the New Zealand Security Intelligence Service.

(3) Accordingly, a specified individual who already has a current electronic identity credential at the time the new identity information is created may, on application under **section 24**, be issued another electronic identity credential in respect of his or her new identity.

(4) If **subsection (3)** applies and the other electronic identity credential is issued, the specified individual may choose to use either or both of the electronic identity credentials in question.

(5) However, a specified individual who does not have a current electronic identity credential at the time the new identity information is created may, on application under **section 24**, be issued an electronic identity credential in respect of—
- (a) his or her original identity; or
- (b) his or her new identity; or
- (c) both identities.

(6) If **subsection (5)(c)** applies and 2 electronic identity credentials are issued, the specified individual may choose to use either or both of the electronic identity credentials in question.

(7) A specified individual who uses either or both of the specified individual's electronic identity credentials as contemplated by **subsections (4) and (6)** is not excused from any criminal liability in respect of any act or omission involving the use of those credentials that would otherwise constitute an offence against any other enactment.

(8) However, **subsection (7)** does not limit or affect the provision of any other enactment or rule of law that confers protection on a specified individual against criminal liability and

if there is any inconsistency between that subsection and that provision, the latter prevails.

(9) In this section,—

(a) **Director of Security** has the meaning given to it by section 2 of the Births, Deaths, Marriages, and Relationships Registration Act 1995; and

(b) **employee**, **officer**, and **undercover Police officer** have the meanings given to them by section 65(5) of that Act.

13 Limits of exception in section 12

(1) To avoid doubt, the following individuals for whom new identity information has been created under section 65 of the Births, Deaths, Marriages, and Relationships Registration Act 1995 do not come within the exception set out in **section 12**:

(a) an individual who is, has been, or will be a witness in any proceeding and who is not a specified individual:

(b) an individual who needs protection because of his or her relationship to an individual who is, has been, or will be a witness in any proceeding.

(2) For an individual referred to in **subsection (1)**, the chief executive—

(a) may, on application under **section 24**, issue an electronic identity credential in respect of the individual's new identity; and

(b) if applicable, must cancel, in accordance with **section 29**, an electronic identity credential that has been issued in respect of the individual's original identity.

14 Electronic identity credential to be personal to individual

An electronic identity credential is personal to the individual to whom it has been issued and may not be transferred or vest by operation of law in any person other than that individual.

15 Individual has no property rights in electronic identity credential

To avoid doubt, an individual does not have any legal or beneficial interest in an electronic identity credential that has been issued to him or her.

Use of electronic identity credential

16 Restrictions on use of electronic identity credential

(1) An individual may use an electronic identity credential only if it has been issued to him or her and only while it is current.

(2) To avoid doubt, a parent or guardian of a child under 14 years of age must not use an electronic identity credential that has been issued to the child except when acting on behalf of the child.

17 How individual may use electronic identity credential

(1) An individual may use an electronic identity credential—

(a) that has been issued to him or her; and

(b) that is current; and

(c) for the purpose of verifying his or her identity by electronic means in order to meet the identification requirements of a participating agency in relation to any applicable transaction or service.

(2) An individual may, subject to this Act, do all or any of the following:

(a) obtain access to—

(i) the core identity information contained in the individual's electronic identity credential:

(ii) the information referred to in **paragraph (b)** of the definition of associated information in **section 7** (that is, information about the status of the individual's electronic identity credential):

(b) request the Service under **section 26(1)(d)** to correct or update the core identity information referred to in **paragraph (a)(i)**:

(c) give consent for the Service to supply to a participating agency, as the case may be, all or any of the core identity information referred to in **paragraph (a)(i)** for the purpose of verifying the individual's identity.

18 Use of electronic identity credential by participating agency

(1) The Service may supply any of the following information to a participating agency if the participating agency has paid or

has made arrangements to pay any fees or charges prescribed by regulations made under this Act or set by an agreement referred to in **section 66(4)(a)(ii) or (b)(ii)**:

(a) core identity information contained in an individual's current electronic identity credential:

(b) information derived from, or based on, core identity information referred to in **paragraph (a)** (for example, the individual's age as derived from his or her date of birth):

(c) associated information.

(2) A participating agency that is supplied by the Service with any of the information referred to in **subsection (1)** may use the information to verify the identity of the individual concerned by electronic means.

(3) For the purposes of **subsections (1) and (2)**, a participating agency may—

(a) choose the types of transactions or services offered by the agency that are to be applicable transactions or services (as long as the choice of those transactions or services is consistent with achieving the purpose of this Act); and

(b) choose the types of core identity information that the agency will accept or require for the purpose of verifying an individual's identity; and

(c) for a continuing service, determine the frequency at which an individual will be required to verify his or her identity in order to continue to receive the service from the agency.

(4) This section is subject to this Act and any other enactment.

19 Legal effect of using electronic identity credential

(1) A legal requirement for an individual to supply information about the individual's identity to a participating agency is met by the individual giving consent for the Service to supply, as the case may be, all or any of the core identity information contained in the individual's current electronic identity credential to the participating agency.

(2) A legal requirement to supply information about an individual's identity includes, for example, a legal requirement for the information when the individual is—

(a) making an application:
(b) making or lodging a claim:
(c) lodging a return:
(d) making a request:
(e) lodging an objection:
(f) making a complaint.

(3) A legal requirement for an individual to provide a signature to a participating agency is met by the individual giving consent for the Service to supply the individual's current electronic identity credential to the participating agency in circumstances where—

(a) the individual adequately indicates his or her approval of information (besides his or her core identity information) provided in relation to an applicable transaction or service; and
(b) if the purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of such approval can be detected.

(4) **Subsection (1) or (3)** applies to a legal requirement to supply information or, as the case may be, to provide a signature even if the information or signature is required to be supplied or provided in some other specified manner.

(5) **Legal requirement**—

(a) means a requirement that is in an enactment administered by a participating agency or is otherwise imposed under the general law; and
(b) includes a provision that sets out consequences that depend on whether or not the provision is complied with.

20 Effect of change in status of electronic identity credential on applicable transactions or services completed or provided before change occurred

(1) A change in status of an electronic identity credential does not, of itself, affect the validity of any applicable transaction

or service that was completed or provided before the change even if the identity of the individual to whom the transaction or service relates was verified using the credential.

(2) Nevertheless, the chief executive—

(a) must give written or electronic notice of the revocation of an electronic identity credential to each participating agency with which an individual has used the credential; and

(b) may provide information about any other change in the status of an electronic identity credential to a participating agency with which an individual has used the credential if, in the chief executive's opinion, it is in the participating agency's interest to receive that information.

(3) **Subsection (1)** is subject to any direction that a court may give under **section 60(1)(c)**.

21 Access to record of usage history

(1) Only the following persons may access the record of usage history for an individual:

(a) the individual to whom the electronic identity credential that is the subject of the record has been issued:

(b) a law enforcement agency that satisfies the chief executive that access to the record is required to avoid prejudice to the investigation or prosecution of a specified offence:

(c) a person who satisfies the chief executive that access to the record is required for the conduct of proceedings before a court or tribunal relating to electronic identity credentials or the Service:

(d) a person who satisfies the chief executive that information obtained from accessing the record is to be used only for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the subject of the information:

(e) a person authorised by the chief executive who is carrying out administrative, technical, or other functions relating to the management, maintenance, and use of the Service.

(2) **Subsection (1)(b)** does not prevent, limit, or affect—
  (a) the issue by a District Court Judge of a search warrant under section 198 of the Summary Proceedings Act 1957 in respect of the record of usage history; or
  (b) the execution of the warrant in respect of the record.

(3) For the purposes of **subsection (1)(d)**, the chief executive—
  (a) must ensure that the record of usage history is made available only in a form that protects the privacy of the individual concerned; and
  (b) may, for that purpose, aggregate information before it is made available under that subsection.

(4) Despite **subsection (1)**, the chief executive may refuse access to the record of usage history if the chief executive considers that—
  (a) access to the record may prejudice an investigation or prosecution against an individual for a specified offence; or
  (b) access to the record may prejudice the security and integrity of the Service; or
  (c) access to the record cannot be given for technical or practical reasons.

(5) This section overrides the Official Information Act 1982.

Applications for electronic identity credential

22 What application may be made

An application to the chief executive may be made for an electronic identity credential—
  (a) to be issued under **section 24**; or
  (b) to be renewed under **section 25**; or
  (c) to be amended under **section 26**; or
  (d) to be voluntarily cancelled under **section 27**.

23 Who may make application

(1) An individual—
  (a) may make an application on his or her own behalf; but
  (b) must not make an application for someone else (except as provided in **subsection (2)(a)**).

(2) If the individual is a child under 14 years of age, the application—

(a) must be made by the child or the child's parent or guardian; and

(b) if made by the child, must include the written or electronic consent of at least 1 of the child's parents or guardians.

24 Application for issue

(1) An application for an electronic identity credential to be issued must—

(a) be made in a manner approved by the chief executive under **section 41**; and

(b) include any information specified by the chief executive under **section 42**; and

(c) include any other prescribed information or documentation; and

(d) be accompanied by the prescribed fee (if any).

(2) The chief executive may grant the application only if—

(a) the application complies with **subsection (1)**; and

(b) the chief executive is satisfied from the information included with the application, or from a comparison of the information undertaken in accordance with **section 35(4)**, or after proper inquiries, that the identity of the applicant has been authenticated; and

(c) **subsection (3)** does not apply.

(3) The chief executive must refuse the application if—

(a) it is made by, or on behalf of, a child under 14 years of age and it does not include the written or electronic consent of at least 1 of the child's parents or guardians; or

(b) the applicant has already been issued with an electronic identity credential and it is suspended under **section 30**; or

(c) an order made by a court under **section 60(1)(a)** in respect of the applicant has not expired; or

(d) the chief executive has not completed any action necessary to give effect to an order made by a court under **section 60(1)(b)**; or

(e) the chief executive knows that the applicant is under investigation, is liable to prosecution, or is the subject of a charge, in respect of a specified offence.

(4) If the chief executive refuses the application, he or she must, as soon as practicable, give the applicant written or electronic notice of the decision and the reason for it.

(5) Despite **subsection (3)(e)**, the chief executive may grant the application even though he or she knows that the applicant is under investigation, is liable to prosecution, or is the subject of a charge, in respect of a specified offence if he or she considers that refusing the application may prejudice the investigation or proceedings into or in respect of the offence.

25 Application for renewal

(1) An application to renew an electronic identity credential may be made either before or after the expiry of the electronic identity credential (as provided in **section 10**).

(2) **Section 24** applies, with any necessary modifications, to the application as if it were an application for an electronic identity credential to be issued.

26 Application for amendment

(1) An application to amend an electronic identity credential may be made if—

(a) an individual has changed his or her name; or

(b) an individual's core identity information has changed as a result of the individual's adoption under any of the following:

(i) an adoption order under the Adoption Act 1955:

(ii) an adoption order that has the same operation and effect as an adoption order under that Act:

(iii) an adoption to which section 17 of that Act or section 11 of the Adoption (Intercountry) Act 1997 applies; or

(c) an individual has assumed and intends to maintain the gender identity of a person of a different sex from the sex that is included in the individual's electronic identity credential; or

(d) an individual considers, on reasonable grounds, that there is an error or omission in the core identity information contained in his or her electronic identity credential.

(2) The application must—
(a) be made in a manner approved by the chief executive under **section 41**; and
(b) include any information specified by the chief executive under **section 42**; and
(c) include any other prescribed information or documentation; and
(d) be accompanied by the prescribed fee (if any).

(3) The chief executive may grant the application only if—
(a) the application complies with **subsection (2)**; and
(b) the chief executive is satisfied from the information included with the application, or from a comparison of the information undertaken in accordance with **section 35(4)**, or after proper inquiries, that good reason for the amendment exists; and
(c) **subsection (4)** does not apply.

(4) The chief executive must refuse the application if it is made by, or on behalf of, a child under 14 years of age and it does not include the written or electronic consent of at least 1 of the child's parents or guardians.

(5) If the chief executive refuses the application, he or she must, as soon as practicable, give the applicant written or electronic notice of the decision and the reason for it.

(6) Despite **subsection (3)**, the chief executive may grant the application even though he or she knows that the applicant is under investigation, is liable to prosecution, or is the subject of a charge, in respect of a specified offence if he or she considers that refusing the application may prejudice the investigation or proceedings into or in respect of the offence.

27 Application for voluntary cancellation

(1) An application for an electronic identity credential to be voluntarily cancelled must—

(a) be made in a manner approved by the chief executive under **section 41**:

(b) be accompanied by the prescribed fee (if any).

(2) If an application complies with **subsection (1)**, the chief executive must—

(a) grant the application; and

(b) give to the applicant, as soon as practicable, written or electronic notice of the cancellation of the applicant's electronic identity credential.

Mandatory amendment or cancellation, suspension, or revocation of electronic identity credential

28 Mandatory amendment of electronic identity credential

(1) The chief executive must amend an electronic identity credential if the chief executive is satisfied, after proper inquiries, that—

(a) the core identity information of the individual to whom it has been issued has changed as a result of the individual's adoption under any of the following:

(i) an adoption order under the Adoption Act 1955:

(ii) an adoption order that has the same operation and effect as an adoption order under that Act:

(iii) an adoption to which section 17 of that Act or section 11 of the Adoption (Intercountry) Act 1997 applies; or

(b) there is an error or omission in the core identity information contained in the electronic identity credential; or

(c) the core identity information contained in the electronic identity credential needs to be updated as a result of information produced by a comparison undertaken in accordance with **section 35(4)**.

(2) **Subsection (1)**—

(a) applies whether or not an application to amend the electronic identity credential is made to the chief executive under **section 26**; and

(b) does not limit the grounds for making an application to amend an electronic identity credential under **section 26**.

(3) If **subsection (1)(b)** applies, the chief executive must remove any incorrect information and replace it with new information, but only if he or she is satisfied that the new information in his or her possession is correct.

29 Mandatory cancellation of electronic identity credential

(1) The chief executive must cancel an electronic identity credential if the chief executive is satisfied, after proper inquiries, that the individual to whom it has been issued—

(a) has died; or

(b) is a specified individual who is exempted under **section 12(1)** from the requirements of **section 11**, but is no longer using the credential because it relates to 1 of his or her identities that is no longer required; or

(c) is an individual referred to in **section 13(1)** and the credential is in respect of his or her original identity.

(2) **Subsection (1)**—

(a) applies whether or not an application to voluntarily cancel the electronic identity credential is made to the chief executive under **section 27**; and

(b) does not limit the grounds for making an application to voluntarily cancel an electronic identity credential under that section.

30 Suspension of processing of application or electronic identity credential

(1) This section applies if—

(a) an individual is under investigation for a specified offence; or

(b) the chief executive has reasonable grounds to believe that an individual is liable to prosecution, or is the subject of a charge, in respect of a specified offence.

(2) The chief executive may suspend, as the case may be,—

(a) the processing of an application relating to the individual; or

(b) the individual's electronic identity credential.

(3) The chief executive may withdraw the suspension at any time by written or electronic notice to the individual concerned if he or she is satisfied that the reason for the suspension no longer applies.

(4) An individual whose electronic identity credential is suspended may not apply for the credential to be renewed or for a further credential to be issued during the period of the suspension.

(5) The suspension of an electronic identity credential does not affect its expiry.

31 Revocation of electronic identity credential

(1) The chief executive may revoke an individual's electronic identity credential if the chief executive is satisfied, after proper inquiries, that the credential—

(a) was issued, renewed, or amended on the basis of any false or fraudulent representation or declaration, made either orally or in writing; or

(b) was issued or renewed in error.

(2) An individual whose electronic identity credential is revoked may apply for another electronic identity credential to be issued to him or her.

32 Process for suspension or revocation

(1) Before exercising the power of suspension conferred by **section 30** or, as the case may be, the power of revocation conferred by **section 31**, the chief executive must give the individual—

(a) written or electronic notice of the proposed suspension or revocation and the reason for it; and

(b) a reasonable opportunity to make written or electronic submissions.

(2) However, **subsection (1)** does not apply if the chief executive considers that giving written or electronic notice to the individual—

(a) may prejudice the investigation referred to in **section 30(1)(a)** or the inquiries referred to in **section 31(1)**; or

(b) is not practicable because the individual cannot be located and his or her contact details cannot readily be established; or

(c) may compromise the security and integrity of the electronic identity credential in question or, as the case may be, of the Service and immediate suspension or revocation is necessary to avoid or lessen that risk.

(3) If the chief executive decides to exercise the power of suspension or revocation after considering the written or electronic submissions (if any) made by the individual, the chief executive must, as soon as practicable, give written or electronic notice of the suspension or revocation to the individual.

(4) The written or electronic notice must specify—

(a) the reason for the suspension or revocation; and

(b) the date on which and the time at which the suspension or revocation commences; and

(c) for a suspension, the period of the suspension.

Subpart 2—Administrative provisions

Information matching

33 Definitions

In **sections 34 and 35**,

identity-related information has the meaning given to it by **section 7**

responsible authority means any of the following, as the case may be:

(a) the Registrar-General:

(b) the chief executive of each department of State that, for the time being, is responsible for the administration of any of the following Acts:

(i) the Citizenship Act 1977:

(ii) the Immigration Act 2009:

(iii) the Passports Act 1992.

34 Purpose of disclosure of identity-related information

The purpose of **section 35** is to facilitate the disclosure of identity-related information to the chief executive and the Service for the purpose of helping the chief executive to—

(a) authenticate an individual's identity; and
(b) keep the core identity information contained in an individual's electronic identity credential accurate and up to date.

35 Disclosure of identity-related information

(1) The chief executive and a responsible authority may enter into an agreement for the disclosure by the responsible authority to the chief executive of identity-related information in respect of an individual who has applied for or been issued with an electronic identity credential.

(2) **Subsection (1)** applies even though the chief executive is the same person as the responsible authority.

(3) A responsible authority may disclose identity-related information only in accordance with an agreement entered into under **subsection (1)**.

(4) The chief executive or the Service may cause a comparison to be made of any identity-related information disclosed under an agreement entered into under **subsection (1)** with information held in the Service database.

36 Use of results of information matching

(1) The chief executive may keep and maintain information produced by a comparison undertaken in accordance with **section 35(4)** for use in auditing the access and use of that information by the Service or employees of the department for the purposes of this Act.

(2) This section applies despite rule 6 of the information matching rules set out in Schedule 4 of the Privacy Act 1993.

Functions of chief executive

37 Functions of chief executive

The functions of the chief executive under this Act are the following:

(a) to establish and maintain the Service database:
(b) to provide advice and information to participating agencies on matters relating to the use of electronic identity credentials:

(c) to enter into and carry out any agreement with a third party under **section 47(1)(b)** for the performance of any function or duty, or the exercise of any power, imposed or conferred on the chief executive by this Act:

(d) to prepare reports required by the Privacy Commissioner under **section 53**:

(e) to perform any other functions and duties and exercise any other powers specified in this Act or in regulations made under this Act:

(f) to administer this Act:

(g) to perform any functions that are incidental and related to, or consequential upon, the functions set out in **paragraphs (a) to (f)**.

Duties of chief executive

38 Chief executive must take all reasonable steps to authenticate individual's identity

(1) The chief executive must take all reasonable steps to ensure that the identity of an individual has been authenticated before an electronic identity credential is issued to the individual.

(2) Without limiting **subsection (1)**, examples of reasonable steps that the chief executive could take to authenticate an individual's identity include the following:

(a) to cause a comparison to be made of any identity-related information disclosed under an agreement entered into under **section 35(1)** with information held in the Service database:

(b) to ask for an identity information check to be carried out in accordance with **Schedule 1**.

39 Chief executive must publish requirements

If the chief executive gives an approval under **section 41** or specifies requirements for information under **section 42**, he or she must publish a notice of the approval or the requirements—

(a) on an Internet site maintained by or on behalf of the chief executive:

(b) by any other means he or she considers appropriate.

40 Chief executive must keep record of usage history

(1) The chief executive must keep a record of the usage history of each electronic identity credential (whether the credential is current or otherwise).

(2) The record of usage history—

(a) must include, subject to **subsection (3)**, information about which participating agency has used an individual's electronic identity credential to verify the identity of the individual; and

(b) must include information about each occasion that any of the persons referred to in **section 21(1)** accesses the record; and

(c) must be available for access at all times by the individual whose electronic identity credential it is (subject to **section 21**); and

(d) may be kept in electronic form so long as it is readily retrievable.

(3) The record of usage history must not include details about any transaction between an individual and a participating agency.

Powers of chief executive

41 Chief executive may approve manner in which applications to be made

(1) The chief executive may approve the manner in which applications must be made.

(2) Without limiting **subsection (1)**, the chief executive may—

(a) allow applications to be lodged electronically or by any other means; and

(b) specify the electronic format for applications that may be lodged electronically.

42 Chief executive may specify what information to be provided with applications

(1) The chief executive may specify what information must be provided with an application.

(2) Without limiting **subsection (1)**, the chief executive may—

(a) issue standard forms (including electronic forms) requiring information or setting out information that must be provided with an application; and

(b) specify requirements in connection with the use of standard forms, including requirements relating to electronic signatures on electronic forms; and

(c) specify what evidence of identity is required to be provided with an application.

(3) Any evidence of identity requirements under **subsection (2)(c)** may apply—

(a) generally or in respect of a specified class or classes of applicants:

(b) differently to different applicants in different circumstances.

(4) Those evidence of identity requirements may also include a requirement that every applicant must submit, or allow the Service to take, a photograph of the applicant.

(5) The chief executive may compare the photograph with information held in the Service database or with information disclosed under an agreement entered into under **section 35(1)** to ensure that the applicant is not—

(a) applying for more than 1 electronic identity credential to be issued to him or her at any given time (subject to **section 12**); or

(b) applying for an electronic identity credential to be issued or renewed on the basis of any false or fraudulent representation or declaration; or

(c) an individual to whom an electronic identity credential must not be issued because of a court order under **section 60(1)(a)**.

(6) A comparison under **subsection (5)** may be carried out manually or electronically (for example, using facial recognition software).

43 Chief executive may set standards or specifications for use of electronic identity credentials by participating agencies

(1) The chief executive may set standards or specifications that participating agencies must comply with in respect of the use of electronic identity credentials by those agencies.

(2) Without limiting **subsection (1)**, the standards and specifications may relate to 1 or more of the following:
- (a) measures to protect the privacy of individuals:
- (b) measures to protect and enhance the security of information supplied to participating agencies:
- (c) minimum requirements for the storage of information supplied by the Service.

44 Chief executive may require participating agencies to report on use of electronic identity credentials

(1) The chief executive may require a participating agency to provide to the chief executive, by a given date and time or at specified intervals, a written or an electronic report on the use of electronic identity credentials by the agency.

(2) Without limiting **subsection (1)**, the chief executive may require the report to include information about 1 or more of the following:
- (a) the numbers and types of applicable transactions or services offered by the participating agency:
- (b) the types of core identity information that the participating agency is accepting or requiring for the purpose of verifying an individual's identity:
- (c) how the participating agency proposes to comply, or is complying, with the standards or specifications set by the chief executive under **section 43**.

(3) The chief executive may also require a participating agency to include an auditor's report on the information contained in the written report.

(4) A participating agency must comply with a requirement made under this section.

45 Chief executive may suspend use of electronic identity credentials by participating agencies

(1) The chief executive may suspend the use of electronic identity credentials by a participating agency if satisfied that—
- (a) the participating agency has failed to comply with—
  - (i) the standards and specifications set by the chief executive under **section 43**:
  - (ii) a reporting requirement under **section 44**; or

(b) the suspension is necessary to protect the security and integrity of the Service in respect of an investigation that it is undertaking into the possible misuse of electronic identity credentials by that participating agency or any other participating agency.

(2) Before exercising the power of suspension conferred by **subsection (1)**, the chief executive must give the participating agency—

(a) written or electronic notice of the proposed suspension and the reason for it; and

(b) a reasonable opportunity to make written or electronic submissions.

(3) However, **subsection (2)** does not apply if **subsection (1)(b)** applies and the chief executive considers that giving written or electronic notice to the participating agency may prejudice the investigation in question.

(4) If the chief executive decides to exercise the power of suspension conferred by **subsection (1)** after considering the written or electronic submissions (if any) made by the participating agency, the chief executive must, as soon as practicable, give written or electronic notice of the suspension to the agency.

(5) The written or electronic notice must specify—

(a) the reason for the suspension; and

(b) the period of the suspension; and

(c) the date on which and the time at which the suspension commences.

(6) Despite the suspension, the participating agency continues to be subject to the provisions of this Act and, among other things, remains liable to pay any outstanding fees or charges prescribed by regulations made under this Act or set by an agreement referred to in **section 66(4)(a)(ii) or (b)(ii)**.

46 Chief executive may delegate functions, duties, and powers

(1) The chief executive may delegate to any person (whether an employee of the State services or not), either generally or particularly, any of the chief executive's functions, duties, and powers under this Act.

(2) However, the chief executive must not delegate any function, duty, or power to a person or class of persons who are employed outside the State services without the written consent of the Minister.

(3) A delegation may be made to—
- (a) a specified person; or
- (b) a person belonging to a specified class of persons; or
- (c) the holder of a specified office or appointment; or
- (d) the holder of an office or appointment of a specified class.

(4) A delegation—
- (a) must be written; and
- (b) may not include a power to further delegate any function, duty, or power; and
- (c) may be made subject to any restrictions and conditions that the chief executive thinks fit; and
- (d) is revocable at any time, in writing; and
- (e) does not prevent the performance of a function or duty, or the exercise of a power, by the chief executive.

(5) A person to whom any functions, duties, or powers are delegated may perform and exercise them in the same manner and with the same effect as if they had been conferred directly by this Act and not by delegation.

(6) A person who appears to act under a delegation is presumed to be acting in accordance with its terms in the absence of evidence to the contrary.

(7) This section does not limit or affect the chief executive's power of delegation under section 41 of the State Sector Act 1988.

47 Chief executive may enter into agreement with third party for performance of functions and duties, or exercise of powers, under this Act

(1) The chief executive may perform his or her functions and duties, or exercise his or her powers, under this Act—
- (a) through the employees of the department:
- (b) by entering into an agreement with a third party (whether corporate or unincorporate).

(2) The chief executive must not enter into an agreement under **subsection (1)(b)** or agree to an extension of the term of an agreement without the written consent of the Minister.

(3) Nothing in this section or in any agreement entered into under **subsection (1)(b)** relieves the chief executive of the obligation to perform any function or duty, or to exercise any power, imposed or conferred on the chief executive by this Act.

48 Application of Ombudsmen Act 1975 and Official Information Act 1982 to certain delegates of chief executive and to certain third parties

(1) This section applies to the following:

(a) a person who is not an employee of the State services to whom the chief executive has delegated, under **section 46(1)**, the chief executive's functions, duties, or powers under this Act:

(b) a third party with whom the chief executive has entered into an agreement under **section 47(1)(b)** for the performance of the chief executive's functions and duties, or the exercise of the chief executive's powers, under this Act.

(2) For the purposes of the Ombudsmen Act 1975 and the Official Information Act 1982, a person or third party to whom this section applies is to be treated as part of the department when performing the chief executive's functions and duties, or exercising the chief executive's powers, under this Act.

Reconsideration of decisions

49 Application of section 50

Section 50 applies to the following decisions that are made by the chief executive:

(a) a decision to refuse to issue an electronic identity credential under **section 24**; or

(b) a decision to refuse to renew an electronic identity credential under **section 25**; or

(c) a decision to refuse to amend an electronic identity credential under **section 26**; or

(d) a decision to refuse to cancel an electronic identity credential under **section 27**; or

(e) a decision to amend an electronic identity credential under **section 28**; or

(f) a decision to cancel an electronic identity credential under **section 29**; or

(g) a decision to suspend the processing of an application under **section 30(2)(a)**; or

(h) a decision to suspend an electronic identity credential under **section 30(2)(b)**; or

(i) a decision to revoke an electronic identity credential under **section 31**; or

(j) a decision to suspend the use of electronic identity credentials by a participating agency under **section 45**.

50 Reconsideration of decision

(1) A person dissatisfied with a decision to which this section applies may apply to the chief executive for a reconsideration of the decision.

(2) An application under **subsection (1)** must be made in a manner approved by the chief executive and, for the purposes of this subsection, **section 41** applies with any necessary modifications.

(3) If the original decision was made by the chief executive personally, it must be reconsidered by the chief executive personally.

(4) If the original decision was made by a person acting under the delegated authority of the chief executive, it must be reconsidered by—

(a) a person not involved in making the original decision; or

(b) the chief executive.

(5) The person undertaking the reconsideration—

(a) may take into account any new or additional information supplied by the applicant for reconsideration; and

(b) must complete the reconsideration within 20 working days after the date on which the chief executive receives the application for reconsideration under **subsection (1)**; and

(c) must, as soon as practicable, give the applicant written or electronic notice of—

(i) the decision on the reconsideration; and

(ii) the reasons for the decision on the reconsideration.

(6) The decision on the reconsideration is final and no further application for reconsideration of that decision can be made.

(7) To avoid doubt, this section does not affect the right of any person to apply, in accordance with law, for judicial review.

Electronic Identity Verification Service

51 Electronic Identity Verification Service

The Electronic Identity Verification Service is the same service as the Identity Verification Service that—

(a) was operating immediately before the commencement of this Act; and

(b) issued pre-commencement electronic identity credentials.

52 Function of Service

(1) The function of the Service is to support the chief executive in performing his or her functions or duties, and in exercising his or her powers, under this Act.

(2) The Service and, in particular, the employees of the department, perform functions or duties, and exercise powers, that the chief executive may from time to time delegate to those employees under **section 46**.

Reporting requirements

53 Privacy Commissioner may require periodic reports on operation of Service or of confirmation agreement

(1) The Privacy Commissioner may, at intervals not shorter than 12 months, require the chief executive to provide the Privacy Commissioner with a report on—

(a) the operation of the Service or any aspect of the Service:

(b) the operation of a confirmation agreement entered into accordance with **Schedule 1**.

(2) Without limiting **subsection (1)(a)**, the Privacy Commissioner may require the chief executive to include information about the following matters in a report under that subsection:
- (a) the number of participating agencies:
- (b) the number of electronic identity credentials that have been issued or cancelled:
- (c) the types of transactions or services for which electronic identity credentials are used:
- (d) the number of times electronic identity credentials have been used by all or any classes of individuals:
- (e) any issues that have arisen, or that are likely to arise, in the use of the Service.

(3) A single report may address the matters in **subsection (1)(a) and (b)** if reports on both of those matters are required by the Privacy Commissioner to be the subject of a report.

Part 3
Miscellaneous provisions

Application of other Acts

54 Application of Official Information Act 1982

(1) Despite anything in the Official Information Act 1982, only the following persons may access a photograph of any individual stored in the Service database:
- (a) the individual who is the subject of the photograph:
- (b) the chief executive or an employee of the Service or department who is authorised by the chief executive for the purpose:
- (c) an officer of a law enforcement agency for the purpose of any proceedings relating to a specified offence.

(2) A person who has access to a photograph under **subsection (1)(b) or (c)** may use the photograph only in the course, and for the purposes, of the person's official duties.

(3) This section is in addition to **sections 21(5) and 48**.

55 Application of Privacy Act 1993

(1) Except as provided in **subsection (2) and section 36(2)**, this Act does not limit or affect the Privacy Act 1993.

(2) Information privacy principle 11 of the Privacy Act 1993 does not apply to personal information held in accordance with the provisions of this Act.

(3) For the purposes of Part 8 of the Privacy Act 1993, a person is taken to have breached an information privacy principle under section 66(1)(a)(i) of that Act if the person contravenes any of **sections 17, 18, and 21** or any other provisions of this Act that—

(a) impose a prohibition or restriction in relation to the availability of personal information; or

(b) regulate the manner in which personal information may be obtained or made available.

(4) To avoid doubt, neither the Service database nor the record of usage history is a public register within the meaning of section 58 of the Privacy Act 1993.

Offences and penalties

56 Offences relating to Service information and material

(1) A person commits an offence who knowingly—

(a) deletes, alters, or copies any information recorded in or on the Service database; or

(b) allows any information recorded in or on the Service database to be deleted, altered, or copied; or

(c) records or stores any information (whether correct or incorrect and including software) in or on the Service database; or

(d) allows any information (whether correct or incorrect and including software) to be recorded or stored in or on the Service database; or

(e) causes the operation of the Service database to—

(i) fail; or

(ii) deny service to any authorised users; or

(iii) provide service to any unauthorised users.

(2) **Subsection (1)** applies to—

(a) the deletion or alteration of information recorded in the Service database, or the recording or storage of information in the Service database, whether it is achieved directly or by altering or damaging the database, its pro-

gramming, another device, the programming of another device, or any electronic storage; and

(b) the copying of information recorded in the Service database (whether it is achieved directly from the database, by means of another device, by the interception or copying of an electronic message, or from any form of electronic storage).

(3) A person who commits an offence against this section is liable on conviction on indictment to imprisonment for a term not exceeding 10 years, or to a fine not exceeding $250,000, or to both.

57 Offence relating to improper issue of electronic identity credential

(1) A person commits an offence who intentionally or recklessly issues an electronic identity credential to an individual to whom it does not relate.

(2) A person who commits an offence against this section is liable on conviction on indictment to imprisonment for a term not exceeding 10 years, or to a fine not exceeding $250,000, or to both.

58 Offences relating to improper access to and use of core identity information and improper use of electronic identity credential

(1) A person commits an offence who knowingly—

(a) accesses the Service database directly or indirectly to obtain any core identity information contained in an individual's electronic identity credential or any associated information; or

(b) supplies to any other person or otherwise uses or discloses that core identity information.

(2) A person other than a participating agency commits an offence who knowingly asks another person to use an electronic identity credential to verify that other person's identity in relation to any transaction or service (whether the transaction or service is offered online or not).

(3) A person commits an offence who knowingly uses an electronic identity credential that has not been issued to him or her.

(4) A person who commits an offence against this section is liable on conviction on indictment to imprisonment for a term not exceeding 2 years, or to a fine not exceeding $50,000, or to both.

59 Offences involving statements or documentation

(1) A person commits an offence who, in making an application (either for himself or herself, or for a child under 14 years of age),—

(a) makes a written or oral statement knowing that it is false or misleading in a material particular; or

(b) makes a written or oral statement that is recklessly false or misleading in a material particular; or

(c) provides any means of identification knowing that it is false or having reason to suspect that it has been forged or falsified.

(2) A person who commits an offence against this section is liable on conviction on indictment to imprisonment for a term not exceeding 5 years, or to a fine not exceeding $50,000, or to both.

Court orders relating to specified offences

60 Court may make certain orders in relation to specified offence

(1) When sentencing an individual for a specified offence, a court may make all or any of the following orders:

(a) an order that an electronic identity credential must not be issued to the individual, either indefinitely or for any period that may be specified in the order:

(b) an order that an electronic identity credential that has been issued to the individual be revoked:

(c) an order giving any direction that the court thinks fit about the validity of any applicable transaction or service that was completed or provided as a result of, or

in connection with, the commission of the specified offence.

(2) The court may make an order under **subsection (1)(a) or (b)** if satisfied that it is desirable to do so for reasons of the security and integrity of the Service or of the Service database.

(3) An order under **subsection (1)(a) or (b)** may be in addition to, or instead of, any other penalty the court may impose under this Act or any other enactment.

(4) If the court makes an order under **subsection (1)**, the Registrar of the court must ensure that a copy of the order is given to the chief executive within 5 working days after the making of the order.

(5) The chief executive must, as soon as practicable, take any action that is necessary to give effect to the order.

Protection from liability

61 Protection from liability

(1) Neither the chief executive nor any employee or agent of the department is under any criminal or civil liability in respect of any act done or omitted in the course of the performance or exercise or intended performance or exercise of any functions, duties, or powers under this Act.

(2) There is no cause of action against the Crown or a Minister of the Crown, or against any other person, to recover damages for any loss or damage that is due directly or indirectly to the use of an electronic identity credential to verify an individual's identity.

(3) **Subsection (2)** applies whether the loss or damage is caused by any person taking any action or failing to take any action, so long as the act or omission occurred in the performance or exercise of any functions, duties, or powers under this Act.

(4) A person is not exempted from liability under this section for any act or omission to act that constitutes bad faith or gross negligence on the part of that person.

Notices

62 Giving of notices

(1) Any notice or any other document required to be given to any person under this Act, or any regulation made under this Act, may be given by—

(a) delivering it to that person; or

(b) delivering it to that person's usual or last known place of residence or business; or

(c) posting it to that person's usual or last known place of residence or business; or

(d) sending it by fax, if the person has nominated a fax address; or

(e) sending it by email or other similar means of communication, if the person has provided an email or similar address.

(2) A notice or document that is sent to a person at a fax number or an email address must be treated as received by that person not later than 2 days after the date on which it is sent.

(3) A notice or document that is posted to a person must be treated as received by that person not later than 7 days after the date on which it is posted.

(4) However, a notice or document must not be treated as received if the person to whom it is posted or sent proves that it was not received, otherwise than through fault on the person's part.

Regulations

63 Regulations relating to participating agencies

(1) The Governor-General may, by Order in Council, make regulations declaring any of the following to be a participating agency for the purposes of this Act:

(a) a government department named in Part 1 of Schedule 1 of the Ombudsmen Act 1975:

(b) an organisation named in Part 2 of Schedule 1 of the Ombudsmen Act 1975:

(c) a local organisation named in Part 3 of Schedule 1 of the Ombudsmen Act 1975:

(d) any other organisation or agency (whether part of the State services or not):

(e) a statutory office or statutory officer established or appointed by or under an Act administered by a government department, organisation, or agency referred to in **paragraphs (a) to (d)**.

(2) The Governor-General may, by Order in Council, make regulations amending any regulations made under **subsection (1)** to—

(a) add the name of a body, person, or office declared to be a participating agency under that subsection:

(b) omit the name of a participating agency and substitute the name of another participating agency:

(c) omit the name of a participating agency and substitute another name in recognition of a change in the participating agency's name:

(d) omit the name of a participating agency.

(3) Regulations made under **subsection (1)** may specify a particular body, person, or office or a class or classes of bodies, persons, or offices.

(4) Regulations under **subsection (2)(d)** may be made only on the recommendation of the Minister made in accordance with **section 64**.

64 When Minister may recommend certain regulations relating to participating agencies

The Minister may recommend the making of regulations under **section 63(2)(d)** to omit the name of a participating agency if, among other things,—

(a) the agency has persistently failed to comply with—

(i) the standards and specifications set by the chief executive under **section 43**:

(ii) a reporting requirement under **section 44**; or

(b) the agency's use of electronic identity credentials has been suspended by the chief executive for an indefinite period under **section 45**.

65 Regulations relating to agencies for purposes of Schedule 1

(1) The Governor-General may, by Order in Council, make regulations declaring any person or body of persons (whether corporate or unincorporate and whether in the public sector or

private sector) to be an agency for the purposes of **Schedule 1**.

(2) The Governor-General may, by Order in Council, make regulations amending any regulations made under **subsection (1)** to—

(a) add the name of a person or body of persons declared to be an agency under that subsection:

(b) omit the name of an agency and substitute the name of another agency:

(c) omit the name of an agency and substitute another name in recognition of a change in the agency's name:

(d) omit the name of an agency.

(3) Regulations made under **subsection (1)** may specify a particular person or body of persons or a class or classes of persons or bodies.

66 Regulations relating to fees

(1) The Governor-General may, by Order in Council, make regulations prescribing the fees or charges payable to enable the recovery of direct and indirect costs of the department in administering this Act that are not provided for by—

(a) money that is funded by the Crown for the purpose; or

(b) money payable to the chief executive under an agreement entered into under **section 47(1)(b)** or an agreement referred to in **subsection (4)(a)(ii)**.

(2) Examples of the costs that may be recovered include—

(a) the costs of processing applications:

(b) the costs of issuing electronic identity credentials:

(c) the costs of providing, operating, and maintaining the Service, the Service database, or other processes in connection with the administration of this Act.

(3) Regulations made under **subsection (1)** may specify—

(a) the matters for which fees or charges are payable:

(b) the amounts of fees or charges or the method or rates by which they are to be assessed:

(c) the individuals or participating agencies, or classes of individuals or participating agencies, liable for payment of the fees or charges:

(d) the conditions or circumstances for which the fees or charges must be paid:

(e) how the fees or charges are to be paid.

(4) Without limiting **subsection (3)(a)**, regulations made under **subsection (1)**—

(a) may provide that they do not apply to any fees or charges that—

(i) are payable to the chief executive by a participating agency or a class of participating agencies for the use of electronic identity credentials under **section 18**; and

(ii) the chief executive may set in accordance with an agreement between the chief executive and the participating agency or, as the case may be, participating agencies:

(b) do not apply to any fees or charges that—

(i) are payable to a third party by any person other than the chief executive for the performance of any of the chief executive's functions or duties, or the exercise of any of the chief executive's powers, under this Act in accordance with an agreement entered into under **section 47(1)(b)**; and

(ii) may be set by the third party in accordance with a separate agreement between the third party and the other person.

(5) Nothing in **subsection (4)** prevents regulations being made under **subsection (1)** prescribing the fees or charges that are payable for applications to which any of **sections 24(1)(d), 26(2)(d), and 27(1)(b)** apply even though the agreement referred to in **subsection (4)(b)(i)** provides for a third party to perform functions or duties, or exercise powers, in relation to those applications.

67 Other regulations

The Governor-General may, by Order in Council, make regulations—

(a) declaring any government department to be a law enforcement agency for the purposes of this Act:

(b) prescribing, for the purposes of **section 10**, the period of duration of an electronic identity credential:

(c) prescribing any other information or documentation that must be included in an application:

(d) providing for any other matters contemplated by this Act that are necessary for its administration or necessary for giving it full effect.

Transitional provisions

68 Pre-commencement electronic identity credential

(1) This section applies to an electronic identity credential (a **pre-commencement electronic identity credential**) that—

(a) was issued before the date of commencement of this section under an agreement between the department and any individual; and

(b) is current or suspended as at that date.

(2) On and from the commencement of this section, a pre-commencement electronic identity credential must be treated as if it were an electronic identity credential that had been issued under this Act and, subject to **subsection (3)**, the provisions of this Act apply accordingly with all necessary modifications.

(3) A pre-commencement electronic identity credential expires at the time at which it would have expired if this Act had not been enacted.

(4) Without limiting **subsection (2)**, a pre-commencement electronic identity credential may be renewed, amended, cancelled, suspended, revoked, or otherwise dealt with in accordance with this Act.

69 Existing application for pre-commencement electronic identity credential

(1) This section applies to an application for a pre-commencement electronic identity credential to be issued that—

(a) had been received by the Service before the date of commencement of this section; and

(b) had not been granted, refused, or withdrawn before that date.

(2) On and from the commencement of this section, the application must be dealt with as if it were an application for an electronic identity credential to be issued under **section 24**.

70 Pre-commencement third-party agreement

(1) This section applies to an agreement (a **pre-commencement third-party agreement**)—

(a) between the chief executive and a third party for the third party to perform the chief executive's functions and duties, or exercise the chief executive's powers, under this Act; and

(b) that was entered into before the date of commencement of this section; and

(c) that is in force as at that date.

(2) On and from the commencement of this section,—

(a) the pre-commencement third-party agreement must be treated as if it were an agreement entered into under **section 47(1)(b)** (except that **section 47(2)** does not apply); and

(b) a reference in this Act to an agreement entered into under that section must be taken to include a reference to the pre-commencement third-party agreement; and

(c) a reference in this Act to a third party must be taken to include the third party that entered into the pre-commencement third-party agreement.

Consequential amendments

71 Consequential amendments

The enactments specified in **Schedule 2** are consequentially amended as indicated in that schedule.

Schedule 1
ss 38(2), 65

Identity information checks

Contents

Preliminary

1 Purpose of schedule

The purpose of this schedule is to facilitate the authentication of an individual's identity by providing a mechanism for the chief executive to confirm whether an individual's identity information is consistent with any information recorded by an agency.

2 Interpretation

(1) In this schedule, unless the context otherwise requires,—

action—

(a) includes failure to act; and

(b) also includes any policy or practice

adverse action means any action that may adversely affect the rights, benefits, privileges, obligations, or interests of any specific individual

agency means a person or body of persons declared by the Governor-General, by regulations made under **section 65**, to be an agency for the purposes of this schedule

database, in relation to an agency, means any file, register, device, or computer system in or on which information is recorded by the agency

identity information—

(a) means core identity information as defined in **section 7**; and

(b) includes any other information relating to an individual (for example, a document or part of a document relating to the individual) that the individual provides to the Service for the purpose of authenticating the individual's identity with the Service; and

(c) also includes any information about the status of any other recorded information referred to in **paragraph (b)**

identity information check means a check that is carried out for the purpose described in **clause 1**

recorded information means information that is recorded in or on an agency's database.

(2) Any term that is defined in **section 7** and used, but not defined, in this schedule has the same meaning as in that section.

Identity information checks

3 Conditions for carrying out identity information check

(1) An agency may carry out an identity information check for the chief executive if—

(a) the individual who is or will be the subject of the check has consented (in written or electronic form) to the check before it is carried out; and

(b) the chief executive has given the agency an assurance (in written or electronic form) that the individual has consented to the check; and

(c) the chief executive and the agency are parties to a confirmation agreement that complies with **clause 6**; and

(d) the check is carried out in accordance with the agreement; and

(e) the chief executive has paid or has made an arrangement to pay any fees and charges payable under the agreement.

(2) For the purposes of **subclause (1)(a)**, an individual may consent to an identity information check on—

(a) a one-off basis (that is, for each identity information check); or

(b) an ongoing basis (that is, for a series of identity information checks, whether repeated or otherwise).

(3) An individual who consents to an identity information check may withdraw the consent before—

(a) the check is carried out, in the case of a consent given on a one-off basis; or

(b) all of the checks, or any further checks, are carried out, in the case of a consent given on an ongoing basis.

4 How identity information check is carried out

(1) In order for an identity information check to be carried out by an agency, the chief executive must submit an individual's identity information to the agency by any electronic or other means specified in the relevant confirmation agreement.

(2) On receiving the individual's identity information, the agency must carry out a search of its database for any recorded information about the individual.

(3) If it is impracticable for the agency to comply with **subclause (2)** for any reason, the agency must advise the chief executive that the identity information check cannot be carried out and may ask the chief executive to resubmit the individual's identity information.

(4) The agency must not, at any stage, supply to the chief executive any recorded information about the individual who is the subject of the search.

(5) However, **subsection (4)** does not limit or prevent the disclosure of any information about the status of any recorded information in relation to the individual.

(6) After carrying out the search referred to in **subclause (2)**, the agency must supply to the chief executive information about the search result and, in particular, whether any or all of the

individual's identity information submitted to the agency is consistent with any recorded information.

(7) Without limiting **subclause (6)**, the information that may be supplied under that subclause generally includes, subject to **subsection (4)**, one of the following search results:

Result	Description
Consistent	Identity information is consistent with recorded information
Not consistent	Identity information is not consistent with recorded information
Exception	Information about the status of recorded information is available

(8) For the purposes of **subclauses (6) and (7)**, identity information may be treated as consistent with recorded information despite any variation between them because of pronunciation or punctuation.

Confirmation agreements

5 Parties to confirmation agreement

The chief executive may enter into a confirmation agreement with any agency.

6 Form and content of confirmation agreement

(1) A confirmation agreement must be in writing.

(2) A confirmation agreement must—

(a) state the purpose of the agreement; and

(b) specify which database it applies to.

(3) In addition, a confirmation agreement must specify the following terms or conditions:

(a) the conditions for carrying out identity information checks, including the conditions specified in **clause 3**; and

(b) the manner in which the chief executive may obtain an individual's consent for an identity information check; and

(c) the circumstances in which an individual's consent for an identity information check that is given on an ongoing basis must be treated as having expired; and

(d) the procedures that the chief executive must follow before taking adverse action against an individual as a result of carrying out an identity information check, including the requirement to give the individual a reasonable opportunity to make submissions or to be heard; and

(e) an alternative process for dealing with an individual whose identity information cannot be confirmed using an identity information check because, for example, there is no recorded information about the individual or the individual has not given his or her consent to an identity information check; and

(f) the fees and charges payable for identity information checks and the manner in which those fees and charges are to be paid; and

(g) the grounds on which the agreement may be terminated; and

(h) the process that must be followed by the parties before exercising any right to terminate the agreement; and

(i) the process for monitoring the parties' compliance with the terms or conditions of the agreement, including the requirement for the parties to keep, for monitoring purposes, records in respect of identity information checks and the requirement to provide those records to the Privacy Commissioner if requested; and

(j) the requirement that the chief executive must consult the Privacy Commissioner about the terms or conditions of confirmation agreements, including the consultation requirements in **clause 7**.

(4) A confirmation agreement may specify any other terms or conditions that the parties consider to be appropriate.

(5) A confirmation agreement may specify different terms or conditions from those contained in another confirmation agreement even though the agencies concerned belong—

(a) in the same class; or

(b) in different classes.

(6) A confirmation agreement may be varied by further agreement between the parties.

7 Standard terms or conditions for confirmation agreement

(1) The chief executive may develop standard terms or conditions for a confirmation agreement that apply, or are proposed to apply, to particular agencies or classes of agencies, but must consult the Privacy Commissioner before or while doing so.

(2) If the chief executive is proposing to enter into a confirmation agreement that will contain terms or conditions that are materially different from the standard terms or conditions developed under **subclause (1)**, the chief executive may develop alternative terms or conditions for the proposed agreement, but must consult the Privacy Commissioner about those terms or conditions before entering into the agreement.

(3) If the chief executive is proposing to vary a confirmation agreement by amending any terms or conditions developed under **subclause (1) or (2)** that are contained in the agreement, the chief executive must consult the Privacy Commissioner about the proposed amendments to those terms or conditions before varying the agreement.

(4) However, the requirement to consult the Privacy Commissioner under **subclause (3)** does not apply if the variation relates to—

(a) the fees and charges payable under the agreement; or

(b) terms or conditions that are minor or incidental in nature.

(5) If **subclause (1) or (2)** does not apply, the chief executive must consult the Privacy Commissioner about the terms or conditions of a confirmation agreement.

8 Periodic review of terms or conditions of confirmation agreements generally

(1) The Privacy Commissioner may, at intervals not shorter than 12 months, require the chief executive to—

(a) review the terms or conditions of any confirmation agreement (whether or not they are standard terms or conditions developed under **clause 7**); and

(b) report on the outcome of the review to the Privacy Commissioner.

(2) If, after a review under **subclause (1)**, the Privacy Commissioner and the chief executive agree that amendments to the terms or conditions of a confirmation agreement are required, the chief executive must vary the confirmation agreement to include the amendments to the terms or conditions.

(3) To avoid doubt, a variation to a confirmation agreement under **subclause (2)** applies only if the agency that is party to the agreement agrees to it.

9 Fees and charges payable under confirmation agreement

A confirmation agreement may require the chief executive to pay fees and charges to an agency for carrying out identity information checks.

Information requirements

10 List of agencies

The chief executive must publish a list of agencies that are party to a confirmation agreement on an Internet site maintained by or on behalf of the chief executive in an electronic form that—

(a) is publicly accessible (at all reasonable times); and

(b) is free of charge.

Schedule 2

s 71

Consequential amendments

Part 1
Amendments to Acts

Privacy Act 1993 (1993 No 28)

Schedule 3: insert in its appropriate alphabetical order:

Electronic Identity Verification Act 2011	**Section 35**

Summary Proceedings Act 1957 (1957 No 87)

Part 2 of Schedule 1: insert its appropriate alphabetical order:

Electronic Identity Verification Act 2011	**56**	Offences relating to Service information and material
	57	Offence relating to improper issue of electronic identity credential
	58	Offences relating to improper access to and use of core identity information and improper use of electronic identity credential
	59	Offences involving statements or documentation

Part 2
Amendment to regulations

Customs and Excise Regulations 1996 (SR 1996/232)

Regulation 74(3)(b): revoke and substitute:

"(b) any of the following:

"(i) a passport:

"(ii) a New Zealand driver licence:

"(iii) a current electronic identity credential issued to the applicant (if applicable in terms of the **Electronic Identity Verification Act 2011**):

Part 2—*continued*

Customs and Excise Regulations 1996 (SR 1996/232)—*continued*

"(iv) any other form of official identification bearing a photo of the applicant that is acceptable to the chief executive as a comparable form of official identification."

Wellington, New Zealand:
Published under the authority of the New Zealand Government—2011