

EXPLANATORY STATEMENT

Telecommunications Act 1997

Telecommunications (National Broadband Network—Restricted Recipients and Storage, Handling and Destruction of Protected Carrier Information) Rules 2008 (No. 1)

Issued by the authority of the Minister for Infrastructure, Transport, Regional Development and Local Government, on behalf of the Minister for Broadband, Communications and the Digital Economy in accordance with an authorisation under section 18C of the *Acts Interpretation Act 1901*

The *Telecommunications (National Broadband Network—Restricted Recipients and Storage, Handling and Destruction of Protected Carrier Information) Rules 2008 (No. 1)* (the Rules) are made by the Minister for Infrastructure, Transport, Regional Development and Local Government under subsections 531N(1) and 531P(1) of the *Telecommunications Act 1997* (the Act). Sections 531N and 531P of the Act are contained in Part 27A of the Act, which was inserted into the Act by the *Telecommunications Legislation Amendment (National Broadband Network) Act 2008*.

Background and legislative basis

Part 27A of the Act

Part 27A of the Act sets out a scheme for specified information to be provided by specified telecommunications carriers to the Commonwealth and for such information to be provided to companies that are considering making or intending to make a submission in response to a request for proposals issued by the Commonwealth for the creation or development of a new open access, high speed broadband network (known as the National Broadband Network). A Request for Proposals in respect of the National Broadband Network was released by the Commonwealth on 11 April 2008.

Under section 531C of the Act, the Minister has the power to make a disallowable non-legislative instrument specifying the particular information to be provided by specified carriers to ‘authorised information officers.’ The term ‘authorised information officer’ is defined in the Act to mean the Secretary of the Department, a Deputy Secretary of the Department, an SES employee of the Department whose duties relate to the National Broadband Network Taskforce or a person appointed by the Minister under section 531M of the Act to be an authorised information officer. Section 531F of the Act requires a specified carrier to provide the specified information within the period specified in the instrument made by the Minister under section 531C.

Information provided by carriers in compliance with section 531F is ‘protected carrier information’ for the purposes of Part 27A. Division 3 of Part 27A imposes on recipients of protected carrier information express prohibitions in relation to the disclosure and use of protected carrier information, except as permitted by the provisions in Part 27A.

Under subsection 531H(1) of the Act, an authorised information officer may disclose protected carrier information to persons who are ‘entrusted company officers’ of companies that are considering making or intending to make a submission in response to a request for proposals, referred to in the Act as a ‘designated requested for proposal notice’, issued by the Commonwealth for the creation of the National Broadband Network. Under subsection 531K(2) of the Act, an entrusted company officer may disclose protected carrier information to another entrusted company officer for certain permitted purposes, including for the purpose of deciding whether to make a submission in response of a designated request for proposal notice or to prepare such a submission.

Part 27A was enacted in recognition of the importance of maximising the competitive tension in the Request for Proposals process for the National Broadband Network, for which it is essential to make available to proponents in the process certain network information held by carriers to enable the development of robust proposals.

Restricted Recipients and Storage, Handling and Destruction of Protected Carrier Information Rules

The Rules comprise restricted recipients rules for the purposes of subsection 531N(1) of the Act and rules relating to the storage, handling and destruction of protected carrier information for the purposes of subsection 531P(1) of the Act.

Restricted recipients rules

Clause 4 of the Rules specifies the entrusted company officers to whom protected carrier information may be disclosed by an authorised information officer under subsection 531H(1) or by an entrusted company officer under paragraph 531K(2)(a) of the Act. Clause 4 has the effect of restricting the individuals to whom protected carrier information may be disclosed and who would otherwise fall within the definition of ‘entrusted company officer’ in section 531B of the Act.

The rules in clause 4 are supplementary to the overarching non-disclosure obligations and restrictions on use imposed upon recipients of protected carrier information by Part 27A of the Act. Disclosure of protected carrier information by an authorised information officer under subsection 531H(1) to an entrusted company officer other than a receiving officer as defined in the Rules would be a contravention of section 70 of the *Crimes Act 1914*. Disclosure of protected carrier information by a receiving officer or entrusted company officer under paragraph 531K(2)(a) to an entrusted company officer in relation to whom the requirements in paragraphs 4(2)(a) and (b) have not been met would be a contravention of a civil penalty provision (subsection 531K(4)). This could result in a pecuniary penalty of up to \$50,000.

Storage, handling and destruction rules

Clauses 5 to 9 of the Rules specify the obligations of recipients of protected carrier in relation to protected carrier information, including rules about the storage of the information, both in electronic and hard copy form, rules about the handling of protected carrier information including the manner in which it is transported or transmitted between entrusted company officers, rules specifying administrative

procedures for recording all disclosures of the information and the manner in which information may be incorporated into other documents. These Rules are intended to ensure that there are appropriate security measures and procedures in place to prevent unauthorised access to and disclosure of protected carrier information that has been disclosed to companies that are considering or intending to make a proposal in response to the request for proposals for the National Broadband Network.

Subsection 531P(3) of the Act requires a person to comply with rules in force under subsection 531P(1) (i.e. the rules in clauses 5 to 9 of the Rules). Subsection 531K(4) prohibits a person from aiding, abetting, inducing or being knowingly involved in a contravention of proposed subsection 531P(3). Subsections 531P(3) and (4) are civil penalty provisions (subsection 531P(5)). Failure to comply with a rule in clauses 5 to 9 of the Rules may result in the imposition of a civil penalty of up to \$50,000 in the case of an entrusted company officer or up to \$250,000 for a relevant company.

These Rules are a legislative instrument for the purposes of the *Legislative Instruments Act 2003*. The Attorney-General's Department and national security agencies were consulted on a draft of the Rules and were broadly supportive of these Rules. A draft of the Rules was also published on the Department of Broadband, Communications and the Digital Economy's website on 18 July 2008. The Department wrote to carriers and proponents in the National Broadband Network competitive assessment process on 21 July 2008 and invited their comments on the draft Rules. A number of submissions were made in relation to the draft Rules and the comments on the draft Rules were taken into account by the Minister for Infrastructure, Transport, Regional Development and Local Government before the making of the Rules, on behalf of the Minister for Broadband, Communications and the Arts.

Details of the Rules

Details of the accompanying Rules are set out in the [Attachment](#).

ATTACHMENT

Details of the Telecommunications (National Broadband Network—Restricted Recipients and Storage, Handling and Destruction of Protected Carrier Information) Rules 2008 (No. 1)

Clause 1 – Name of Rules

Clause 1 provides that the title of the Rules is the *Telecommunications (National Broadband Network—Restricted Recipients and Storage, Handling and Destruction of Protected Carrier Information) Rules 2008 (No. 1)*.

Clause 2 – Commencement

Clause 2 sets out the date on which the Rules commence. The Rules commence on the day after they are registered on the Federal Register of Legislative Instruments.

Clause 3 – Definitions

Clause 3 sets out definitions of terms used in the Rules.

The term Act is defined to mean the *Telecommunications Act 1997*.

The term ‘authorised entrusted company officer’ means an entrusted company officer in relation to whom the requirements under subclause 4(2) of the Rules have been met and to whom protected carrier information may be disclosed under subsection 531K(2A) of the Act .

The term, ‘Department’ is defined to mean the Department administered by the Minister which is currently the Department of Broadband, Communications and the Digital Economy. The term ‘Minister’ is defined to mean the Minister administering the Act, who is currently the Minister for Broadband, Communications and the Digital Economy.

The term ‘Determination’ is defined to mean the *Telecommunications (National Broadband Network) Determination under subsection 531H(4) 2008 (No. 1)*.

The term ‘relevant company’ means a company in relation to which a receiving officer has obtained or will obtain protected carrier information under section 531H of the Act. The rules in clauses 5 to 9 impose a number of obligations on a relevant company in relation to the storage, handling and destruction of protected carrier information.

The term ‘receiving officer’ is defined to have the same meaning as in the *Telecommunications (National Broadband Network) Determination under subsection 531H(4) 2008 (No. 1)*. The term is also defined to include an entrusted company officer nominated to replace an existing receiving officer and who meets the requirements specified in the definition to ensure, in the event that a receiving officer ceases employment with a company or the duties of the receiving officer change such that it is no longer appropriate for that person to continue to perform that role, there

is a mechanism available to a company to nominate a replacement receiving officer. The requirements set out in the definition that must be met in order for an entrusted company officer to be considered to be a receiving officer are consistent with the requirements that apply to the initial nomination of a receiving officer (as set out in clause 4 of the Determination) and which an authorised information officer must be satisfied have been met before disclosing protected carrier information under subsection 531H(1) of the Act. It is intended that there would only be one receiving officer at any particular time for a company (see also the note to paragraph 4(1)(a) of the Determination) and that the initially nominated receiving officer would continue to be subject to the obligations in these Rules until such time as the nomination of the replacement receiving officer takes effect (which could not occur before the time that all of the requirements in the definition regarding a replacement receiving officer have been met).

Note 1 to clause 3 highlights that a number of terms which are used in the Rules and are defined in section 531B of the Act have the same meaning in the Rules as they have in the Act, namely ‘authorised information officer’, ‘entrusted company officer’, and ‘protected carrier information’.

Note 2 to clause 3 specifies that the terms ‘document’ and ‘record’, which are used in the Rules, have the same definition as those in the *Acts Interpretation Act 1901* (the AIA).

The term ‘document’ is defined under section 25 of the AIA to include any:

- (a) paper or other material on which there is writing;
- (b) paper or other material on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; and
- (c) article or material from which sounds, images or writings are capable of being reproduced with or without the aid of any other article or device.

The term ‘record’ is defined under section 25 of the AIA to include information stored or recorded by means of a computer.

Clause 4 – Access to protected carrier information

Clause 4 limits the entrusted company officers to whom protected carrier information may be disclosed under subsection 531H(1) and paragraph 531K(2)(a) of the Act.

The effect of subclause 4(1) is that an authorised information officer may only disclose protected carrier information under subsection 531H(1) to an entrusted company officer who is a receiving officer of a company. This would be an entrusted company officer who is a director or employee of a company that has notified that it is considering or intending to lodge a proposal in response to the request for proposals for a National Broadband Network and who has given an authorised information officer an undertaking in substantially the form specified in Schedule 1 to the Determination (see the definition of ‘receiving officer’ in clause 3 and clause 4 of the Determination).

The effect of subclause 4(2) is that only an authorised entrusted company officer may have access to protected carrier information. Subclause 4(2) provides that protected carrier information may be disclosed to an entrusted company officer under

paragraph 531K(2)(a) of the Act if a receiving officer has certified to an authorised information officer that:

- (a) the duties of the entrusted company officer are directly relevant to the exceptions to the prohibition on use of protected carrier information as set out in subsection 531K(2A) the Act; and
- (b) the entrusted company officer has signed an undertaking that is substantially in the form specified in Schedule 1 to the Rules.

The certification would need to be in the form of a statutory declaration made under the *Statutory Declarations Act 1959* (subclause 4(3)). A declaration must be in the prescribed form and be made before a prescribed person (see the *Statutory Declarations Regulations 1993*).

The restriction of the entrusted company officers to whom protected carrier information may be disclosed applies to a disclosure by a receiving officer (who will be the entrusted company officer who receives protected carrier information from an authorised information officer on behalf of a company) and also to all subsequent disclosures by authorised entrusted company officers who have received protected carrier information (whether from the receiving officer or another authorised entrusted company officers).

The purpose of the ‘need to know’ requirement in paragraph 4(2)(a) is to ensure that protected carrier information is only disclosed to entrusted company officers who have a genuine need to access the information having regard to the nature of their duties having regard to the purposes for which protected carrier information may be used as permitted by subsection 531K(2A). These purposes generally relate to use in connection with the National Broadband Network request for proposal process, including use to enable the company to consider whether to lodge a proposal in response to the request for proposals, use in connection with the preparation of such a proposal and, if required during a later stage of the process, use in connection with consideration of whether to vary a proposal or to prepare such a proposal (see paragraph 531K(2A)(a)). It is these purposes that will be of greatest relevance for a receiving officer to determine that the duties of a particular entrusted company officer are directly relevant to the permitted uses in subsection 531K(2A). However, in some instances, the permitted uses provided for in paragraphs 531K(2A)(b) to (d) may also be relevant.

The primary purpose of the undertaking required by paragraph 4(2)(b) is to encourage authorised entrusted company officers’ awareness of their obligations under the Rules and the Act.

The note after subclause 4(2) clarifies that a certification under subclause 4(2) may relate to more than one entrusted company officer and that a receiving officer may make more than one certification. Subclause 5(2) of the Rules requires a receiving officer to keep the original of all undertakings signed by entrusted company officers.

Clause 5 – Receiving officer to maintain list of officers who are given access to protected carrier information and relevant company to provide access to premises on request

The purpose of subclause 5(1) is to ensure that a comprehensive and auditable list is created and maintained by a receiving officer regarding each authorised entrusted company officer to whom protected carrier information is disclosed by the receiving officer and the overall period during which that officer had access to the protected carrier information. This list is required to also include details of the premises where the protected carrier information disclosed by the receiving officer is stored and it would need to be updated if different or additional premises for the storage of protected carrier information are notified under subclause 7(11). The list compiled in accordance with subclause 5(1) is intended to assist in the management and control of the dissemination and use of protected carrier information. It also enables the relevant company and the Commonwealth to promptly identify where the information is stored, thereby facilitating any physical site inspections the relevant company or the Commonwealth may wish to undertake.

Subclause 5(2) requires a receiving officer to keep the original of all undertakings signed by entrusted company officers for the purposes of paragraph 4(2)(b).

Under subclause 5(3), a receiving officer is required to provide to an authorised information officer details about the authorised entrusted company officers to whom the receiving officer has disclosed protected carrier information, the premises where that protected carrier information is stored or the undertakings given by authorised entrusted company officers. Also, if requested, a receiving officer must provide copies of the signed undertakings. A receiving officer is required to comply with such requests as soon as practicable.

Subclause 5(4) requires a relevant company, if requested to do so, to provide the Commonwealth or its authorised agent with the right to access and inspect the premises detailed in the list kept by the receiving officer to ensure that appropriate security arrangements are in place at those premises.

Clause 6 – Storage of protected carrier information

Clause 6 specifies rules regarding the storage of protected carrier information in electronic and hard copy form that apply to all authorised entrusted company officers of a company and are intended to reduce the risk of unauthorised access to protected carrier information. These rules apply not only to the way in which protected carrier information received initially by the company that gave the notice under paragraph 531H(1)(b) is stored, but also extends to the way in which such information is stored by authorised entrusted company officers who are advisers to the company or, in the case where the company is part of a consortium, by authorised entrusted company officers who are from other companies or bodies politic forming part of that consortium.

Subclauses 6(1) and (2) deal with the electronic storage of protected carrier information in electronic form. Subclause 6(3) deals with the physical storage of protected carrier information in hard copy and physical electronic form.

The rules in subclause 6(1) are intended to reduce the risk of unauthorised access to protected carrier information. Subclause 6(1) requires a relevant company to ensure that protected carrier information in electronic form is stored on a separate, stand-alone computer system such that it is quarantined from the company's ordinary business information system. The stand-alone computer system must have no connectivity to the company's business system or other external systems including the Internet. Transfer of protected carrier information from one computer on the stand-alone network to another computer on that network would be permitted and such communications would not need to be encrypted (see subclause 7(10)).

If protected carrier information needs to be sent electronically between the relevant company's premises, it would be possible for this to occur in compliance with the Rules by copying the relevant information stored in the stand-alone system to a storage device such as a USB thumb drive and then accessing the information on the device using a computer connected to the Internet to send the email. The email communication would need to be encrypted in accordance with the requirement in subclause 7(9). The email could be received by a computer connected to the Internet in the other premises and the protected carrier information copied to another electronic storage device in order to enable storage at that premises on a stand-alone system. The authorised entrusted company officers sending and receiving the emails would need to ensure that the protected carrier information is deleted from the computers used to send and receive the emails, so that the protected carrier information is not stored on those computers.

Subclause 6(1) makes it clear that only authorised entrusted company officers can have access to the stand-alone computer system.

Subclause 6(2) sets out rules regarding electronic access to protected carrier information. Such access is to be by way of a system that requires users to be uniquely identifiable and authenticated on each occasion of access. Subclause 6(2) provides for user authentication to be provided for by a variety of means as listed in subclause 6(2).

Subclause 6(3) requires hard copies of protected carrier information or CDs, DVDs, USB thumb drives or other electronic storage devices containing protected carrier information to be securely stored in at least a Security Construction and Equipment Committee (SCEC) Class C container. The hard drives of computers forming part of a stand-alone system for the purposes of subclause 6(1) are not required to be stored in this manner as this would be impractical. A note to subclause 6(3) explains the characteristics of Class B, Class C and Class D containers and the differences between them. The effect of subclause 6(3) is that only Class C and Class B containers can be used to store protected carrier information in hard copy form or that is contained in a CD, DVD or USB thumb drive. If protected carrier information has been stored on a CD, DVD, USB thumb drive or other electronic storage device to enable that information to be transferred or transported between authorised entrusted company officers, the information must be encrypted in accordance subclause 7(9) (see further the discussion in relation to subclause 7(9) below).

Clause 7 - Handling of protected carrier information

Clause 7 sets out rules relating to the handling of protected carrier information. The rules are intended to provide a framework to assist companies that receive protected carrier information, and their authorised entrusted company officers, protect against unauthorised use or disclosure of protected carrier information. Similarly to clause 6, these rules apply not only to the way in which protected carrier information received initially by the company that gave the notice under paragraph 531H(1)(b) is handled, but also extends to the way in which such information is stored by authorised entrusted company officers who are advisers to the company or, in the case where the company is part of a consortium, by authorised entrusted company officers from other companies or bodies politic forming part of that consortium.

Subclause 7(1) requires a relevant company to ensure that protected carrier information is marked 'Strictly Private and Confidential'. Subclause 7(2) specifies how this marking should be applied. Where the information is in hard copy, the marking is to be applied at the top and at the bottom of each page of a hard copy of the information. Where the information is in electronic form, the marking is to be applied in the title and body of the information.

In addition to the obligations of a receiving officer to maintain a list of authorised entrusted company officers to whom the receiving officer has disclosed protected carrier information and the premises at which such information is located (see clause 5), a relevant company must also maintain records of each authorised entrusted company officer who had access to the protected carrier information following the initial disclosure by a receiving officer in accordance with subclause 4(2), the premises where the information is stored and the overall period during which that officer had access to the information (see subclause 7(3)).

In circumstances where copies or extracts are produced of protected carrier information, a relevant company must maintain records of any copies, including screen prints, and extracts of protected carrier information (see subclause 7(4)). Such records must include details of who made the copy or extract, the time and date on which the copy or extract was made, and the time and date on which the copy or extract was destroyed (see subclause 8(5)). This applies in relation to all authorised entrusted company officers and is not limited to copies or extracts made by the officers included in the list referred to in subclause 7(3).

Subclause 7(6) requires a relevant company to ensure that a copy or extract of protected carrier information to be marked with the name or identifiable code of the authorised entrusted company officer who produced it. Subclause 7(6) is expressed to be subject to subclause 7(8). This is to make it clear that in circumstances where protected carrier information has been incorporated into a database or document, it is not necessary for the incorporated information to indicate the name or identifiable code of the person who did this. However, subclause 7(8) would require that the incorporated information be identified in the database or document as protected carrier information and the relevant company would need to ensure that it has a record (whether at an appropriate place in the database or document or in a separate record) of the authorised entrusted company officer who had incorporated the protected carrier information into the database or document.

Subclause 7(7) provides that, in circumstances where material qualities of the whole or part of protected carrier information have been incorporated into a database or document, a relevant company must ensure that the incorporated information is subsequently destroyed or otherwise dealt with in accordance with clause 8. Subclause 7(8) provides that a relevant company must maintain a record of any database or document into which protected carrier information has been incorporated. In addition, such a database or document must contain notes or markings to identify where the information has been incorporated.

The requirements in subclauses 7(7) and (8) are intended to apply where protected carrier information has been incorporated into a database or document in such a way that the incorporated information is still separately identifiable as protected carrier information. These clauses would not apply in circumstances where databases or documents have been produced or derived from protected carrier information but it is not possible to identify or extract protected carrier information from that database or document. For example, a proposal in response to the Request for Proposals for the National Broadband Network that contains information that has been derived from protected carrier information but does not enable the actual protected carrier information to be identified would not be covered by subclauses 7(7) or (8). However, to the extent that protected carrier information is identifiable from the proposal, then the proposal would be covered by these subclauses and the disclosure of that information to the Commonwealth through the proposal would be authorised by paragraph 531K(2)(b) of the Act.

The rules in subclauses 7(9), 7(10) and 7(11) deal with the transfer of protected carrier information from one authorised entrusted company officer to another.

Subclause 7(9) requires protected carrier information in electronic form that is to be transferred or sent electronically from one authorised information officer to another to be encrypted in accordance with a cryptographic protocol that meets the requirements in ACSI 33 when in transit. How electronic transmission from a stand-alone system can be achieved is discussed in relation to subclause 6(1) above. Subclause 7(9) would also apply where a copy of protected carrier information is to be physically transported from one premises of a relevant company (by copying the information to a USB thumb drive from the stand-alone computer system) to another premises so that the information can be stored and used on a separate stand-alone computer system. The note to subclause 7(9) explains that, for the purposes of ACSI 33, protected carrier information is considered to be classified as “In-Confidence.” ACSI 33 is the Australian Government Information and Communications Technology Security Manual. Further information about ACSI 33 can be found at www.dsd.gov.au.

Subclause 7(10) provides that subclause 7(9) does not apply where protected carried information in electronic form is transferred or sent between authorised entrusted company officers using the same stand-alone computer system referred to in subclause 6(1). For example, it would not be necessary to encrypt an email containing protected carrier information sent from one computer on a stand-alone system to another computer on that system.

Subclause 7(11) deals with the physical transfer of protected carrier information that is in hard copy or electronic form (in a CD, DVD or USB thumb drive) between one authorised entrusted company officer to another. In the circumstances where the other officer is located at the same premises at which the protected carrier information is stored, the information is to be passed by hand (i.e. the officer himself or herself is to give the information to the other officer). In the circumstances where the other officer is not located at the same premises at which the protected carrier information is stored, the information is to be passed by hand or sent by registered courier and, in both instances, is to be double bagged (i.e. enclosed in at least two envelopes). The note to subclause 7(11) highlights the requirement in subclause 7(12) to notify the Commonwealth if protected carrier information is to be stored at premises other than those that have been listed for the purposes of subclause 5(1) or paragraph 7(3)(b) or subparagraph 4(1)(a)(i) of the Determination.

Subclause 7(12) requires a relevant company to notify the Commonwealth if it proposes to store or handle protected carrier information in a location different from the premises recorded under subclause 5(1) or paragraph 7(3)(b), or subparagraph 4(1)(a)(i) of the Determination, must be notified in writing to the Commonwealth. In such cases, the company, if requested, must permit the Commonwealth or an authorised agent of the Commonwealth to inspect the proposed location to ensure that appropriate security arrangements are in place at that location before protected carrier information is moved to that location (see subclause 7(13)). Similarly, a relevant company must, if requested, permit the Commonwealth or an authorised agent of the Commonwealth to inspect premises listed for the purposes of subclause 5(1) or paragraph 7(3)(b) or subparagraph 4(1)(a)(i) of the Determination (see subclause 7(15)). Such requests must be complied with as soon as practicable after the request is made. A relevant company would need to ensure that it has appropriate arrangements in place with its advisers and, if the company is part of a consortium, with the other members of the consortium to enable such inspections to occur if requested.

Subclause 7(14) provides that, if requested, a receiving officer must, as soon as practicable after the request is made, provide an authorised information officer with details of the records mentioned in subclauses 7(3), (4) and (8).

Clause 8 - Destruction of protected carrier information

Clause 8 specifies the circumstances in which protected carrier information is to be destroyed or returned to the Commonwealth and, if so, the manner of destruction. These rules apply not only in relation to protected carrier information received initially by the company that gave the notice under paragraph 531H(1)(b), but also the protected carrier information stored by authorised entrusted company officers who are advisers to the company or, in the case where the company is part of a consortium, from another company or a body politic forming part of that consortium.

Subclause 8(1) provides that if a notice in relation to the destruction of protected carrier information is given by the Commonwealth to a relevant company, the relevant company must destroy or, if applicable return, the information within 1 month of receiving the notice. Subclause 8(1) also specifies the particular manner in which

destruction is to occur and the circumstances in which information is to be returned to the Department for destruction depending on the form of the information:

- (a) all hard copies of protected carrier information and documents into which such information has been incorporated must be shredded in a SCEC (Security Construction and Equipment Committee) endorsed Class 'B' cross-cut paper shredder or disposed by an 'ASIO-endorsed' waste disposal company. The incorporation of protected carrier information into documents is discussed in relation to subclauses 7(7) and (8) above. Note 1 to paragraph 8(1)(a) explains that there are two types of cross-cut shredders, that is, Class 'A' and Class 'B' shredders and their characteristics. Note 2 paragraph 8(1)(a) notes that details of 'ASIO endorsed' waste disposal companies can be obtained from an authorised information officer;
- (b) all CDs or DVDs containing protected carrier information must be returned to the Department for secure destruction; and
- (c) all electronic storage devices (including hard drives and USB thumb drives) on which protected carrier information has been stored must be sanitised in accordance with ACSI 33. A note to paragraph 8(1)(c) explains that for the purposes of ACSI 33, protected carrier is considered to be classified as "In-Confidence." ACSI 33 is the Australian Government Information and Communications Technology Security Manual. Further information about ACSI 33 can be found at www.dsd.gov.au.

The requirements in subclause 8(1) are subject to subclause 8(2), which provides that a relevant company may retain board minutes and any reports that contain protected carrier information to the extent that the company is required to do so by law or any professional standard applicable to the company. This exception is intended to apply to the company that gave the notice under paragraph 531H(1)(b) and, because of the definition of entrusted company officer in section 531B of the Act, advisers to the company or, in the case where the company is part of a consortium, another company or a body politic forming part of that consortium.

In addition to the physical measures that are required to be undertaken for the physical destruction, return or sanitisation of protected carrier information or media in which such information is stored, subclause 8(3) requires a receiving officer to provide a certification to an authorised information officer that the officer's company has complied with the destruction, return, and/or sanitisation (as applicable) obligations set out in subclause 8(1). This certification would need to cover the all protected carrier information disclosed between authorised entrusted company officers of the company, including such officers who are advisers to the company or, in the case where the company is part of a consortium, who are from another company or body politic forming part of that consortium. The certification would also need to be in the form of a statutory declaration made under the *Statutory Declarations Act 1959*. A declaration must be in the prescribed form and be made before a prescribed person (see the *Statutory Declarations Regulations 1993*).

Subclause 8(5) requires a relevant company, if requested, to permit the Commonwealth or an authorised agent of the Commonwealth to inspect any place

protected carrier information has been stored to verify the company's compliance with any request to destroy or return the protected carrier information to the Commonwealth. This rule requires a relevant company to ensure that it has appropriate arrangements in place with its advisers and, if the company is part of a consortium, with the other members of the consortium to enable such inspections to occur if requested.

Clause 9 – Notification and assistance

Subclause 9(1) requires a receiving officer to notify the Commonwealth in writing of any breaches of the Rules by a relevant company or by an entrusted company officer or any breach of an undertaking by the receiving officer under paragraph 4(20)(b) of the Determination or of an undertaking referred to in paragraph 4(2)(b) by an authorised entrusted company officer.

If requested, a receiving officer and an entrusted company officer must give the Commonwealth or an authorised representative of the Commonwealth reasonable assistance (at no cost to the Commonwealth) to ensure that the intention and requirements of the Rules are being duly met. Such assistance could include but is not limited to signing and producing documents.

Schedule 1

Schedule 1 specifies the form of undertaking for the purposes of paragraph 4(2)(b) of the Rules.