**EXPLANATORY STATEMENT**

**Select Legislative Instrument No. 26, 2015**

**National Security Information (Criminal and Civil Proceedings) Regulation 2015**

The *National Security Information (Criminal and Civil Proceedings) Regulation 2015* is made under the *National Security Information (Criminal and Civil Proceedings) Act 2004*.

**Overview of the Regulation**

The *National Security Information (Criminal and Civil Proceedings) Regulation 2015* (the Regulation) ensures the continuing existence of a pre-existing framework for the protection of national security information in federal criminal proceedings and civil proceedings in which the *National Security Information (Criminal and Civil Proceedings) Act 2004* (the Act) is used. The Regulation replaces the current regulation, the *National Security Information (Criminal and Civil Proceedings) Regulations 2005*, which is due to sunset on 1 April 2015 in accordance with the *Legislative Instruments Act 2003*. The Regulation updates the regulation made in 2005 to make the requirements easier to understand and more accessible to users. The protection measures in the Regulation are substantially the same as those provided in the 2005 regulation.

**Purpose**

The Regulation prescribes, for the purposes of the Act, the requirements for accessing, storing, handling, destroying and preparing security classified documents and national security information in federal criminal proceedings and civil proceedings to which the Act applies. It also prescribes the form of a notice of expected disclosure for the purposes of paragraphs 24(2)(a) and 38D(3)(a) of the Act.

**Framework for the protection of national security information**

The Act was introduced in 2004 to provide a framework for the protection of national security information in federal criminal proceedings and civil proceedings while ensuring the proper administration of justice in those proceedings. The Act implemented recommendations of the Australian Law Reform Commission’s report *Keeping Secrets: The Protections of Classified and Security Sensitive Information (ALRC 98)*. This report recommended the development of a specific Act to deal with the protection of sensitive information in court proceedings. The Act has been used in all key counter‑terrorism prosecutions to date.

The Act needs to be ‘invoked’ in a proceeding before the protection measures in the Act apply. In federal criminal proceedings the prosecutor can invoke the Act by giving notice in writing to the defendant, the defendant’s legal representative and the court that the Act applies to the proceeding. In a civil proceeding, the Act is invoked by the Attorney‑General (or a Minister appointed by the Attorney‑General where the Attorney‑General is a party to the proceeding) by giving notice in writing to the parties to the proceeding, the legal representatives of the parties and the court that the Act applies to the proceeding. Unless and until this notice is given the Act will not apply to the court proceeding.

The Act and regulations made under it provide comprehensive measures for the protection of national security information in court proceedings. While the Act sets out if and how information may be disclosed in court proceedings, the regulations detail how parties to the proceedings need to treat national security information to ensure it is appropriately protected. Section 49 of the Act provides that the Governor‑General may make regulations prescribing matters required or permitted by the Act to be prescribed, or necessary or convenient to be prescribed for carrying out or giving effect to the Act. Subsections 23(1) and 38C(1) of the Act provide that the regulations may prescribe:

* the ways in which national security information that is disclosed, or is to be disclosed, in proceedings must be stored, handled or destroyed, and
* the ways is which, and places at which, such information may be accessed and documents or records relating to such information may be prepared.

The Act is designed to provide as much flexibility to the court and parties as possible. Accordingly, if parties wish to enter into their own arrangement on how to appropriately protect national security information they can do this under section 22 or 38B of the Act. The Attorney‑General is a party to the proceeding for the purposes of these arrangements, which are given effect by a court order. Where the court has given effect to an arrangement by making an order, the Regulation does not apply to that information.

The Regulation will ensure the continued protection of national security information in court proceedings while balancing the proper administration of justice.

**Explanation and effect of provisions**

**Part 1 – Preliminary**

**Section 1 - Name**

This section provides that the name of the instrument is the *National Security Information (Criminal and Civil Proceedings) Regulation 2015*.

**Section 2 – Commencement**

This section provides that the Regulation commences on the day after it is registered.

**Section 3 – Authority**

This section specifies that the Regulation is made under the Act.

**Section 4 – Schedules**

This section provides that each instrument specified in Schedule 1 and Schedule 2 is amended or repealed as set out in the applicable items to the relevant Schedule. Any item in Schedule 1 and Schedule 2 has effect according to its terms.

**Section 5 – Purpose and application**

This section provides for the purpose of the Regulation and the relationship between the Regulation and orders made by a court under section 22 or 38B of the Act.

For the purposes of subsections 23(1) and 38C(1) of the Act, paragraph (1)(a) prescribes the requirements for accessing, storing, handling and destroying security classified documents and national security information, and the requirements for preparing documents that relate to security classified documents or national security information.

For the purposes of paragraphs 24(2)(a) and 38(3)(a) of the Act paragraph (1)(b) prescribes the form of the notice of expected disclosure. Under the Act a specified person must inform the Attorney‑General if that person knows or believes he or she will disclose national security information. The notice must be in the prescribed form, which is provided by the Regulation. Paragraph (1)(c) of the Regulation also prescribes related matters.

Subsection (2) clarifies that the Regulation does not apply to a security classified document or national security information that is the subject of an order that is in force under section 22 or 38B of the Act. In accordance with subsections 23(2) and 38C(2) of the Act, where such an order is in force any regulations made under subsections 23(1) or 38C(1) do not apply.

The note to this section is intended to remind authorised recipients that it is an offence to contravene a requirement of the regulations made under either of sections 45A or 46FA of the Act where that contravention is likely to prejudice national security.

**Section 6 – Definitions**

This section provides the definitions of key terms in the Regulation. The note to this section clarifies that a number of terms used in the Regulation are not defined in the Regulation because they are defined in the Act.

One of the key terms defined by this section is ‘authorised recipient’. An authorised recipient is a person to whom the requirements of the Regulation apply. It is not the intention of the Regulation to limit who can access national security information. The definition of authorised recipient reflects this intention by specifying that a person will be given access to particular national security information and security classified documents by a mechanism other than the Regulation.

The definition provides that an authorised recipient in relation to a particular security classified document or national security information is a person in a proceeding to whom the document or information has been disclosed to in the proceeding in accordance with another mechanism of the Act, an order or process of the court in the proceeding, or with the written authorisation of the Attorney‑General or a representative of the Attorney‑General in the proceeding. In order to receive approval from the Attorney‑General, or a representative of the Attorney‑General, a person may be required to enter into an arrangement with the Australian Government agency owner of the information for the purposes of Part 6, Division 1 of the *Intelligence Services Act 2001*. Judicial officers, which are defined by the Regulation to mean a magistrate or a judge, are specifically excluded from this definition as it is not the place of the Regulation to impose requirements on this category of persons.

Another key term defined by this section is ‘security classified document’. A security classified document is a document which contains national security information that is disclosed, or is to be disclosed, in the proceeding. The document itself does not have to be disclosed in the proceeding (although the definition will capture these documents), but the information in the document must be information that is disclosed, or is to be disclosed in the proceeding. The definition is designed to capture not only those documents that have already been created, but also documents that are created from existing security classified documents or national security information. For example, the definition will capture notes created by legal representatives from national security information, including national security information communicated verbally in the proceeding. Any document created from a security classified document or national security information will need to be treated by the authorised recipient as a security classified document in accordance with the Regulation.

**Section 7 – References to federal criminal proceeding or civil proceeding**

This section provides that a reference in the Regulation to a federal criminal proceeding is a reference to a federal criminal proceeding to which the Act applies. Similarly, a reference in the Regulation to a civil proceeding is a reference to a civil proceeding to which the Act applies.

**Part 2 – Protection of security classified documents and national security information**

**Section 8 – Creation or preparation of documents relating to security classified documents or national security information**

This section places requirements on an authorised recipient in relation to the creation or preparation of documents relating to a security classified document or national security information. It is necessary to place requirements on these documents because the document that is created or prepared will contain sensitive information that requires protection in the same manner as the originating document or information.

Paragraph (1)(a) provides that the section applies to an authorised recipient in relation to a security classified document who creates or prepares a document that includes information in the security classified document. Similarly, paragraph (1)(b) provides that the section also applies to an authorised recipient in relation to national security information that is disclosed, or is to be disclosed, in the proceeding, who creates or prepares a document that includes that information. For example, the section could apply to a legal representative of a defendant who creates notes containing national security information from information disclosed orally by the defendant to that legal representative. These paragraphs also apply to court records made under subsections 29(5) or 38I(5) of the Act. These records are made in relation to closed hearings under the Act where the court determines if national security information is to be disclosed in the proceeding and in what form.

If an authorised recipient prepares a document of the type in subsection (1), subsection (2) provides that the document must be created or prepared in a discrete area.

Subsection (3) provides that if the document is created or prepared in electronic form the authorised recipient must do so on approved information and communications technology equipment.

Subsection (4) provides that the authorised recipient must ensure that the document is assigned a security classification that is the same as the most highly classified information in the document. For example, if a document created by an authorised recipient contains national security information, some of which is classified as Protected and some as Secret, the document must be classified as Secret. Subsection (5) provides that the security classification assigned to the document must be clearly recorded at the top and bottom of each page of the document. Subsection (6) provides that if the authorised recipient has any doubt about the security classification that should be assigned to the document the authorised recipient must consult with the Commonwealth as to the appropriate security classification that should be assigned to the document.

**Section 9 – Copying security classified documents**

This section places requirements on an authorised recipient in relation to the copying of security classified documents. The term ‘copy’ is defined expansively in section 6 to mean recording or reproducing information in any medium. This will include printing a document in electronic form in hard copy. It is necessary to provide protection requirements on copying documents as the unfettered copying of sensitive information increases the risk that the information will be inappropriately disclosed or accessed.

Subsection (1) provides that an authorised recipient must not copy a security classified document or any part of the document, or any national security information in the document, except for the purposes of creating or preparing a document in accordance with section 8. For example, it may be necessary to copy extracts of a security classified document for the purposes of preparing a submission to the court.

Subsections (2) and (3) provide the mechanism for obtaining copies of security classified documents. Subsection (2) allows an authorised recipient to request, in writing, the Attorney‑General or a representative of the Attorney‑General to provide copies of the document. The number of copies requested, the name of the authorised recipient making the request, and the full name of each person who is to be given a copy of the document must be specified in the request under subsection (3).

**Section 10 – Storage of security classified documents in hard copy form**

This section places requirements on an authorised recipient in relation to storing security classified documents in hard copy form. The appropriate storage of security classified documents in hard copy is a key safeguard in ensuring that the document and the information contained in the document is not inappropriately accessed. For example, if a highly classified document is left on a legal representative’s desk overnight there is an increased risk that someone other than an authorised recipient for the document or a judicial officer will access the document.

Subsection (1) provides that an authorised recipient must store a security classified document in hard copy in a locked Class B security container. A Class B security container is defined in section 6 to mean a security container that is fitted with an Security Construction and Equipment Committee (SCEC) endorsed combination lock.

Subsection (2) provides that the combination to the security container must not be known to any person other than an authorised recipient in relation to all security classified documents (and not just some of the documents) stored in the container and to an APS employee whose duties include responsibilities relating to the container. It is necessary to allow certain APS employees to have the combination in case the authorised recipient loses or forgets the combination, and so that the container may be opened if it is provided back to the Commonwealth in accordance with section 18.

Subsection (3) provides that, subject to subsection (4), the security container must be located in a security classified document storage area. A security classified document storage area is defined in section 6 and means an area in which entry and openings are secured at all times to limit access to those persons specified in the definition. Subsection (4) provides that if any security classified documents stored in the security container are classified as Top Secret or Codeword material, the security container must be located in an area approved by the Commonwealth for the purposes of storing such documents. An area approved by the Commonwealth is likely to have increased protection measures in place to ensure that the highly sensitive information contained in the Top Secret or Codeword documents is not inappropriately accessed.

Subsection (5) provides that a person must not remove a security classified document from the security container unless the person is an authorised recipient in relation to the document and needs to remove the document for the purposes of the proceeding or is a judicial officer. A person must also not remove a security classified document from the security container that is located in an area approved by the Commonwealth for storing Top Secret and Codeword material unless the person is permitted by the Commonwealth to access the area.

Subsection (6) provides that if an authorised recipient in relation to a security classified document that is classified as Top Secret or Codeword material removes the document from the security container the authorised recipient must record, in writing, details of the removal, including the recipient’s full name, date and time the document was removed, and the place to where the document is to be taken. This record must be stored in the security container. The purpose of this subsection is to ensure the location of highly classified documents is tracked and the documents are able to be accounted for. The subsection will apply to the authorised recipient who removes such a document other than for the purpose of transferring the document to another authorised recipient in relation to the document. Where the document is transferred to another authorised recipient the authorised recipient must record the relevant details of the transfer in the classified document register. The note to this subsection seeks to ensure that authorised recipients are aware of this requirement.

**Section 11 – Storage and transmission of security classified documents or national security information in electronic form**

This section places requirements on an authorised recipient in relation to the storage and transmission of security classified documents or national security information in electronic form. Similar to section 10, requirements need to be placed on security classified documents and national security information in electronic form to ensure the information is not inappropriately accessed or disclosed. For example, a security classified document should not be stored on information and communications technology equipment other than equipment that has the necessary protections.

Subsection (1) provides that an authorised recipient must not store or transmit a security classified electronic document or national security information in electronic form except where it is on information and communications technology equipment supplied, or approved, by the Commonwealth for the document or information. Paragraph (1)(b) also provides that if a document or information is transmitted it must be transmitted by and to approved information and communications technology for the document or information.

Given the sensitivity of the document or information on the approved information and communications technology equipment, subsection (2) provides that the equipment must be stored in a locked Class B security container when it is not being used. For example, a laptop computer containing an electronic version of a security classified document must be stored in a locked Class B security container when not in use. Paragraph (2)(a) provides that the security container must be located in a security classified document storage area. If the equipment is too large to be stored in a Class B security container, paragraph (2)(b) provides that the equipment must be located in a security classified document storage area. Paragraph (2)(b) may be relevant for items such as large printers.

Subsection (2) has effect subject to subsection (3). Subsection (3) provides that the Commonwealth may require further protection measures for the storage of approved information and communications technology equipment on which a security classified document or national security information that is classified as Top Secret or Codeword material is stored on, or transmitted by or to. Such equipment must be located in an area approved by the Commonwealth for the purpose of storing documents or information with that security classification.

Similar to the requirements in section 10, subsection (4) provides that the Class B security container in which the equipment is stored (subject to paragraph (2)(b)) must have a combination that is not known to any person other than an authorised recipient in relation to all (and not just some) of the security classified documents or national security information stored in the container, or an APS employee whose duties include responsibilities relating to the container.

Subsection (5) provides that the information and communications technology equipment on which the security classified document or national security information is stored or transmitted by or to must not be accessed or removed from the security container except by an authorised recipient in relation to the document or information or a judicial officer. Further, the subsection also provides that if the equipment is in a Commonwealth approved area for the purpose of storing documents or information classified as Top Secret or Codeword only a person who is permitted by the Commonwealth to access the area is able to remove the equipment from a security container.

Subsection (6) provides that the password (if the equipment is capable of being secured by a password) for the approved information and communications technology equipment on which the document or information is stored or transmitted by or to must not be known by a person other than an authorised recipient in relation to all security classified documents or national security information stored in or transmitted by the equipment, or an APS employee whose duties include responsibilities relating to the container.

Subsections (7) and (8) provide an accountability measure for Top Secret or Codeword material in electronic form stored on, or transmitted by or to, approved information and communications technology equipment where that equipment is stored in a Class B security container. If the authorised recipient removes such equipment that recipient must make a written record of their full name, the date and time the equipment was removed and the place to where the equipment is to be taken. The record containing this information must be stored in the security container.

**Section 12 – Handling security classified documents**

This section places requirements on an authorised recipient in relation to handling security classified documents. The handling of a classified document essentially means using or developing that document. For example, the development of a submission to the court containing national security information will be captured by this section. Protection measures need to be placed on handling security classified documents to ensure they are not handled in a manner that has an unacceptable risk that the document will be inappropriately accessed. For example, it would not be appropriate for a person to read a security classified document classified as Secret on a public bus.

Subsection (1) provides that an authorised recipient in relation to a security classified document may only handle the document for the purpose of the proceeding to which the document relates. Subsection (2) further provides that, except for the purpose of carrying the document or using it in court, the authorised recipient may only handle the document in a discrete area. A ‘discrete area’ is defined in section 6 and means an area within an enclosed building or office where public access is restricted, access by employees controlled, and access by visitors strictly controlled and on a needs basis. If the security classified document is classified as Top Secret or Codeword material the document must be handled in an area approved by the Commonwealth for the purpose of handling documents or information with that security classification when not being carried or used in court.

Subsection (3) provides that when handling the document the authorised recipient must ensure that the document cannot be viewed by any person other than an authorised recipient in relation to the document or a judicial officer.

**Section 13 – Handling approved information and communications technology equipment**

This section places requirements on an authorised recipient in relation to the handling of approved information and communications technology equipment. Information and communications technology equipment containing security classified documents or national security information needs to be protected to reduce the risk that a person will access the document or information using the equipment.

Subsection (1) provides that approved information and communications technology equipment on which a security classified document or national security information is stored may only be handled by an authorised recipient in relation to the document or information for the purpose of the proceeding to which the document relates.

Subsection (2) provides that except when the approved information and communications technology equipment is being carried or used in court the equipment can only be handled in a discrete area. If the equipment is being used to store a security classified document or national security information classified as Top Secret or Codeword material that equipment must be handled in an area approved by the Commonwealth for the purpose of handling documents or information with that security classification when not being carried or used in court.

Subsection (3) provides that when handling approved information and communications technology equipment the authorised recipient must ensure that any national security information or security classified documents stored on the equipment cannot be viewed by any person other than an authorised recipient in relation to the document or information or a judicial officer.

**Section 14 – Carrying security classified documents**

This section places requirements on an authorised recipient in relation to carrying security classified documents. Similar to handling documents, the carrying of security classified documents presents a risk that the document will be inappropriately accessed. As such, measures need to be placed on the carrying of these documents to reduce the chance that a person other than an authorised recipient or a judicial officer will access the document.

Subsection (1) provides that an authorised recipient in relation to a security classified document must, when carrying a security classified document in a discrete area, ensure the document cannot be viewed by a person other than an authorised recipient in relation the document or a judicial officer. This would, for example, require a person to cover up the document when carrying it in a discrete area.

Subsection (2) provides that if an authorised recipient is carrying a document other than in a discrete area the document must be inside two SCEC-approved single use bags, in a locked container approved by the SCEC with the keys removed and retained by the authorised recipient, and the document must remain in the custody or control of the recipient. An appropriate container will generally be a SCEC-approved briefcase or bag.

Subsection (3) allows the authorised recipient in relation to the document to give the document to another person for the purpose of carrying the document, but only if that other person is a SCEC endorsed courier, another authorised recipient in relation to the document, or a judicial officer. Subsection (4) provides that if the document is given to a SCEC endorsed courier it must be given to the courier inside two SCEC-approved single use bags.

**Section 15 – Classified document register**

This section places requirements on an authorised recipient in relation to a classified document register. A ‘classified document register’ is defined in section 6 and means a register that includes details of security classified documents that are received, created, prepared or transferred in hard copy form. It is necessary to place requirements on authorised recipients in relation to classified document registers to ensure that security classified documents in proceedings are tracked and accounted for. Classified document registers are used widely by the Commonwealth to keep track of sensitive information.

Subsection (1) provides that an authorised recipient must maintain, or have access to, a classified document register. Subsection (2) provides that as soon as practicable after an authorised recipient receives, creates or prepares a security classified document in hard copy, or transfers the document to another person, the authorised recipient must record the details outlined in paragraphs (a)-(g) in the classified document register. The details in paragraphs (a)-(g) are required to ensure that the security classified document is easily identifiable.

However, despite the requirements in subsection (2), subsection (3) provides that the classified document register must not contain national security information. This is to prevent the inappropriate disclosure of, for example, national security information in the title of the document.

Subsection (4) has been included to clarify that an authorised recipient does not need to comply with subsection (2) if the authorised recipient has already complied with the section when they received, created, or prepared the document and are simply removing the document from the security container referred to in section 10 in which the document is stored and are not transferring the document.

**Section 16 – Security classified documents to remain in Australia**

This section places requirements on an authorised recipient in relation to taking or sending security classified documents or national security information out of Australia.

Taking or sending security classified documents or national security information out of Australia increases the risk that the documents will be inappropriately accessed by a person other than an authorised recipient for the document. Subsection (1) provides that an authorised recipient must not take, or send (including by electronic transmission), security classified documents or national security information out of Australia without the permission of the Commonwealth.

**Section 17 – Return and destruction of security classified documents**

This section places requirements on authorised recipients in relation to the return and destruction of security classified documents. It is intended to apply to those persons who are not bound by archives legislation, such as the legal representative of a defendant or a non‑Commonwealth party to a civil proceeding. The provision is not intended to apply to courts. It is necessary for documents to be destroyed to reduce the number of documents containing sensitive information in existence. The documents only need to be destroyed after proceedings have concluded, although this does not prevent an authorised recipient from returning the document earlier for destruction.

Subsection (1) specifically provides that the section does not apply in relation to security classified documents that are in the possession of a court or a registry of a court. Subsection (2) further provides that the section has effect subject to the *Archives Act 1983* and any equivalent State or Territory legislation. The subsection is not intended to displace archives legislation and the section is not a requirement for the purposes of paragraph 24(2)(a) of the *Archives Act 1983*.

This has been provided to ensure that the Regulation does not provide for the destruction of documents that would otherwise be required to be archived in accordance with applicable archives legislation.

Subsection (3) provides that the authorised recipient who has custody and control of a security classified document that relates to the proceeding must give the document to a representative of the Attorney‑General in the proceeding within 28 days after the conclusion of the proceeding. As per sections 13 and 15 of the Act, the conclusion of the proceeding will include any appeals, re-trials or re-hearings. The authorised recipient must record the transfer of any document to the representative of the Attorney‑General in the classified document register in accordance with section 15. A representative of the Attorney‑General will be such a representative for the purposes of the proceedings.

Subsection (4) provides that if the authorised recipient is a legal representative who has ceased to act for a party in the proceeding, the recipient must, within 28 days after ceasing to act, give the security classified document to a representative of the Attorney‑General in the proceeding or to the new legal representative (if any) of the party. In giving a security classified document to a person under this subsection the authorised recipient must record the transfer of the document in the classified document register in accordance section 15.

Subsection (5) provides that the representative of the Attorney‑General to whom the security classified document is given in accordance with subsection (3) or (4) must ensure the document is destroyed if it is in hard copy. Subsection (6) provides that if the security classified document is given to the representative in electronic form in accordance with subsection (3) or (4), the representative must ensure that the document is deleted from the approved information and communications technology equipment on which it is stored in accordance with Commonwealth requirements and ensure that all record of the document is removed from the equipment, including, if necessary, by destroying all or part of that equipment in accordance with Commonwealth requirements. For example, in order to ensure that all record of a security classified document is removed from a laptop computer it may be necessary to destroy the hard drive of that laptop computer.

Subsection (7) provides that if an authorised recipient gives a security classified document to a representative of the Attorney‑General under subsection (3) or (4) the authorised recipient may view the destruction of the document under subsection (4) or the deletion of the document under subsection (5). This subsection is designed to ensure that, to any extent there is a concern that the Commonwealth may misuse non‑Commonwealth created security classified documents (such as case strategy notes containing national security information), an authorised recipient can view for themselves the destruction or deletion of a security classified document.

**Section 18 – Return of Commonwealth property relating to security classified documents**

This section places requirements on the return of Commonwealth property that has been given to an authorised recipient by the Commonwealth for the purposes of the proceeding. The Commonwealth will continue to provide the necessary equipment for an authorised recipient to comply with the Regulation over the course of the proceeding. However, this equipment should be returned to the Commonwealth once it is no longer need for the proceeding.

This section requires an authorised recipient to return any Commonwealth property relating to a security classified document for the purposes of the proceeding over which the authorised recipient has custody and control. The property must be returned to the Attorney‑General’s Department or a representative of the Attorney‑General in the proceeding within 28 days after the earlier of either the conclusion of the proceeding or, if the authorised recipient is a legal representative who has ceased to act in the proceeding, the authorised recipient ceasing to act in the proceeding.

**Part 3 – Expected disclosure**

**Section 19 – Notice by prosecutor, defendant or defendant’s legal representative of expected disclosure**

This section provides, for the purpose of paragraph 24(2)(a) of the Act, the prescribed form for notice to the Attorney‑General if a prosecutor, defendant, or defendant’s legal representative knows or believes national security information will be disclosed in a federal criminal proceeding. The prescribed form is Form 1 of Schedule 1 to the Regulation.

**Section 20 – Notice by party or party’s legal representative of expected disclosure**

This section provides, for the purpose of paragraph 38D(3)(a), the prescribed form for notice to the Attorney‑General if a party, or a legal representative of a party, knows or believes national security information will be disclosed in a civil proceeding. The prescribed form is Form 2 of Schedule 1 to the Regulation.

**Part 4 – Application and transitional provisions**

**Section 21 – Application of this instrument**

This section provides that the instrument applies in relation to a security classified document that is disclosed, or is to be disclosed, in or for the purposes of a federal criminal proceeding or civil proceeding that had commenced before the commencement of the Regulation but had not been finally determined before commencement, or a federal criminal proceeding or a civil proceeding that is commenced after the commencement of the Regulation. The regulation will also apply to national security information that is disclosed, or is to be disclosed, in a federal criminal proceeding or civil proceeding that had commenced before the commencement of the Regulation but had not been finally determined before commencement, or a federal criminal proceeding or a civil proceeding that is commenced after the commencement of the Regulation.

**Schedule 1 – Forms**

**Form 1 – Notice of expected disclosure of national security information in a federal criminal proceeding**

This form is the prescribed form for the purpose of paragraph 24(2)(a) of the Act.

**Form 2 – Notice of expected disclosure of national security information in a civil proceeding**

This form is the prescribed form for the purpose of paragraph 38D(3)(a) of the Act.

**Statement of Compatibility with Human Rights**

*Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011.*

**National Security Information (Criminal and Civil Proceedings) Regulation 2015**

The *National Security Information (Criminal and Civil Proceedings) Regulation 2015* (the Regulation) is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

**Overview of the regulations**

The *National Security Information (Criminal and Civil Proceedings) Act 2004* (NSI Act) was introduced in 2004 to provide a framework for protecting national security information in federal criminal proceedings and civil proceedings while ensuring the proper administration of justice. The Act implements recommendations of the Australian Law Reform Commission’s report *Keeping Secrets: The Protections of Classified and Security Sensitive Information (ALRC 98)*. This report recommended the development of a specific Act to deal with the protection of sensitive information in court proceedings. The Act has been used in all key counter‑terrorism prosecutions to date.

The NSI Act and regulations made under the Act are designed to provide an overall framework for the protection of national security information in court proceedings while ensuring that preventing the disclosure of this information does not seriously interfere with the administration of justice. While the NSI Act sets out if and how national security information may be disclosed in court proceedings and who can access this information the Regulation details how those persons who are given access need to treat national security information to ensure it is appropriately protected. In particular, the Regulation sets out how those who access national security information in the proceedings can access, store, handle, destroy and prepare national security information. The Regulation also prescribes, for the purposes of paragraphs 24(2)(a) and 38D(3)(a) of the NSI Act, the form of a notice of the expected disclosure of national security information in court proceedings. The Regulation replaces the *National Security Information (Criminal and Civil Proceedings) Regulations 2005*, which is due to expire on 1 April 2015. The new Regulation is designed to update the regulation made in 2005 to make the requirements easier to understand and more accessible to users.

The NSI Act is designed to be as flexible to the court and parties as possible. Accordingly, if parties wish to enter into their own arrangement on how to appropriately protect the information they can do this under section 22 or 38B of the Act. In these cases the Regulation does not apply.

**Human rights implications**

The Regulation seeks to promote the right to a fair trial and a fair hearing. This right is contained in article 14 of the International Covenant on Civil and Political Rights (ICCPR). Under this article all persons shall be equal before the courts and tribunals. Further, in determination of a criminal charge the person has a right to have adequate time and facilities for the preparation of the person’s defence and to communicate with counsel of the person’s own choosing.

The Regulation does not seek to restrict the courts’ power to determine who can access information in a proceeding. Instead, it places appropriate protection mechanisms on any national security information that is disclosed, or is to be disclosed, in the proceeding. The Regulation will give comfort to parties who may be concerned that disclosing national security information in proceedings will result in an inappropriate disclosure of that information. The information protection framework under the Act and the Regulation encourages the disclosure of more information in a proceeding than would otherwise be disclosed without appropriate information protection measures. The Commonwealth, through the Attorney‑General’s Department, will continue to provide any equipment (such as a security container or a secure computer) that a person requires in order to comply with the Act or the Regulation if that person does not already have the equipment.

The Regulation does not place any limitations on the right to privacy. The right to privacy is contained in article 17 of the ICCPR and is the right to have freedom from unwarranted and unreasonable intrusions into activities that society recognises as falling within the sphere of individual autonomy. If private information is also national security information (for example, the name of a security agency employee) the Regulation will ensure protections are placed on this information to prevent its inappropriate disclosure. As such, if the right to privacy is engaged by the Regulation the Regulation may be seen as promoting this right rather than limiting it.

The Regulation also does not place any limitations on the right to freedom of expression. The right to freedom of expression is contained in article 19 of the ICCPR. It is the right to impart ideas by any medium, including written and oral communications. As referred to above, it is ultimately up to the court to decide if and how national security information should be disclosed in the proceeding. The Regulation does not limit the disclosure of information to any person the court has determined should have access to the information.

**Conclusion**

The Regulation is compatible with human rights because it provides protection for Australia’s national security information, and to the extent that it may limit human rights, those limitations are reasonable, necessary and proportionate.

**Consultation**

Consultation on the Regulation was undertaken with key stakeholders. Pursuant to section 17 of the *Legislative Instruments Act 2003* the rule-maker is satisfied that appropriate and reasonably practical consultation has occurred.

Key Government agencies, particularly those which produce and own certain national security information, were consulted in the development of the Regulation. The Commonwealth Director of Public Prosecutions and the Australian Government Solicitor, which both have extensive experience with the NSI Act, were also consulted. Particular consultation was undertaken with:

* Attorney‑General’s Department
* Australian Federal Police
* Australian Government Solicitor
* Australian Geospatial-Intelligence Organisation
* Australian Secret Intelligence Service
* Australian Security Intelligence Organisation
* Australian Signals Directorate
* Commonwealth Director of Public Prosecutions
* Department of Defence
* Department of Foreign Affairs and Trade
* Office of National Assessments