

Crimes Legislation Amendment (Community Safety Orders and Other Measures)
Regulations 2023

EXPLANATORY STATEMENT

Issued by authority of the Attorney-General

in compliance with section 15J of the *Legislation Act 2003*

PURPOSE AND OPERATION OF THE INSTRUMENT

This instrument is made under the *Criminal Code Act 1995* (the Code) and the *Telecommunications (Interception and Access) Act 1979* (the TIA Act).

The *Crimes Legislation Amendment (Community Safety Orders and Other Measures) Regulations 2023* (the Proposed Regulations) are a legislative instrument for the purposes of the *Legislation Act 2003*.

Section 5 of the Code, provides that the Governor-General may make Regulations required or permitted by this Act, or Regulations that are necessary or convenient. The Australian Federal Police (AFP) Minister is the rule-maker for Regulations made under Part 5.3 (Terrorism) and Part 9.10 (Community safety orders) of the Code.

The TIA Act protects the privacy of, and regulates access to, the content of telecommunications and telecommunications data. Section 300 of the TIA Act provides that the Governor-General may make regulations, not inconsistent with the Act, 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.

Part 9.10 (Community safety orders)

Section 395.34 of the Code allows the Court to make specified orders where the serious offender, due to circumstances beyond their control, is unable to engage a legal representative in relation to a CSO proceeding. The Court may make an order staying proceedings for such period, and subject to such conditions as the Court thinks fit, and requiring the Commonwealth to bear all or part of the reasonable costs and expenses of the serious offender's legal representation for the proceeding.

The Proposed Regulations prescribe matters that a Supreme Court of a State or Territory may take into account in determining whether circumstances are beyond a serious offender's control in relation to engaging a legal representative in CSO proceedings under Division 395 of the Code.

Subsections 395.44(1) and (4) of the Code provide for the sharing (requesting and disclosing) of information between the Immigration Minister, and persons prescribed by regulations, to facilitate the administration or execution of Division 395.

The Proposed Regulations amend the listed prescribed persons in the Code Regulations to improve information sharing. Part of the information gathering process would involve the Immigration Minister requesting information from prescribed persons, being Commonwealth and state law enforcement agencies. Agencies' responses to these requests, enables the relevant department to undertake preparatory work to gather evidence for the consideration for the CSOs in relation to CSO-eligible offenders.

This process then informs the Immigration Minister's decision to determine whether to make a CSO application, including mandatory reviews of CSOs. If the Court determines a CSO is required such as a community safety supervision order (CSSO), the relevant department is responsible for providing case management for the serious violent or sexual offender, including costs associated with providing case management services.

The Proposed Regulations are intended to operate in a way that allows the responsible department to request and share information with prescribed persons for the purposes of subsections 395.44(1) and (4) of the Code. The information sharing process assists in obtaining information to conduct a thorough assessment of the risk CSO-eligible offender may impose in committing a serious violent or sexual offence. The Proposed Regulations would improve the efficiency of the information sharing process with relevant agencies, assist in identifying relevant information for CSO considerations, and support case management for serious violent or sexual offenders subject to a CSO. These proposed amendments would also allow the Immigration Minister to request or share information for the administration and execution of Division 395.

Part 5.3 (Terrorism)

Subsections 105A.19(1) and (3) of the Code provide for the sharing (requesting and disclosing) of information between the Attorney-General and persons prescribed in section 10 of the Criminal Code Regulations 2019 (the Code Regulations), to facilitate the execution and administration of Division 105A.

The purpose of the Proposed Regulations is to amend the listed prescribed persons in the Code Regulations to improve information sharing. Part of the information gathering process involves the Attorney-General requesting information from prescribed persons, being

Commonwealth and state law enforcement agencies, and national intelligence agencies. Agencies' responses to these requests, enables the responsible department to undertake preparatory work to gather evidence for the consideration by the Attorney-General of PSOs in relation to eligible terrorist offenders.

The Proposed Regulations will make technical amendments to address three limitations within the Code Regulations (prescribed persons) that have been impacting the information sharing process for the department and partner agencies. The first relates to requests for information from the AFP. Currently, the department is restricted in its ability to only request and share information relating to eligible terrorist offenders with senior executive level AFP employees. This process can be time consuming and delay the sharing of operational information quickly. The proposed amendment would allow sharing with any AFP employee.

The second relates to the Commonwealth's ability to receive information from service providers as prescribed persons. The Commonwealth is responsible for the case management of Victorian ESO matters, however currently only listed prescribed persons such as state or territory agencies can request services providers to provide case management services. The proposed amendment would allow the Commonwealth the same opportunity to obtain assistance from service providers.

The third relates to obtaining information regarding passport cancellations and passport application rejections for relevant eligible terrorist offenders. The Department of Foreign Affairs and Trade (DFAT) is responsible for administering the *Australian Passports Act 2005* (Cth), however, the Code Regulations do not enable the department to request this information from DFAT as the agency is not listed as a prescribed person. The proposed amendment would allow the department to request this information.

The Proposed Regulations would also make minor technical amendments to the Code Regulations to update the reference to the 'Director-General Australian Security Intelligence Organisation' and 'Deputy Director-General of the Australian Security Intelligence Organisation' to 'the Director-General of Security' and 'Deputy Director-General of Security'.

The Proposed Regulations would likely engage a number of human rights, and relevant safeguards are addressed in the Statement of Compatibility.

TIA Regulation Amendments (Community safety orders)

The purpose of the Proposed Regulations is to support the effective operationalisation of the CSO Regime under Division 395 of the Code by ensuring that warrants issued under the TIA Act are issued by issuing authorities in a consistent form containing the requisite information to establish the scope of the warrant.

Amendments to the TIA Regulations are required to support the use of associated law enforcement powers to monitor compliance of a CSSO, protect the community from serious harm by addressing the unacceptable risk of a serious offender committing serious violent or sexual offences or determine whether an application for a Part 9.10 order should be made in relation to an CSO-eligible offender.

Subsection 49(1) of the TIA Act provides that a warrant shall be in accordance with the prescribed form and shall be signed by the Judge or nominated Administrative Appeals Tribunal (AAT) member who issues it.

The Proposed Regulations amend the TIA Regulations to enable the application of telecommunications service warrant forms, named person warrant and warrant for entry on premises and interception of communications forms to be available in relation to CSSO or Part 9.10 order (CSO) applications.

These proposed amendments are consequential to the amendments made by the *Migration and Other Legislation Amendment (Bridging Visas, Serious Offenders and Other Measures) Act 2023*, and ensure that the relevant forms are consistent with the primary legislation, thereby enabling them to be used by an eligible Judge or a nominated AAT member.

The Proposed Regulations amend the TIA Regulations to insert the following Forms of warrants.

- Form 2D: This new form gives effect to proposed subparagraph 46(9)(d)(i) of the TIA Act by providing, as specified by the warrant, the authority for the interception of communications made to or from the telecommunications service with respect to an individual who is subject to a CSSO;
- Form 2E: This new form gives effect to proposed subparagraph 46(9)(d)(ii) of the TIA Act by providing, as specified by the warrant, the authority for the interception of communications made to or from the telecommunications service where a CSSO is in

force in relation to another person, and the particular person is likely to communicate with the other person using the service;

- Form 2F: This new form gives effect to proposed subparagraph 46(12) of the TIA Act by providing, as specified by the warrant, the authority for the interception of communications made to or from the telecommunications service with respect to a person who may be subject to Part 9.10 order (CSO) application;
- Form 4E: This new form gives effect to proposed subparagraph 46A(2E)(e)(i) of the TIA Act by providing, as specified by the warrant, the authority for the interception of communications made to or from telecommunications services that a person who is subject to a CSSO is using or is likely to use;
- Form 4F: This new form gives effect to proposed subparagraph 46A(2E)(e)(ii) of the TIA Act by providing, as specified by the warrant, the authority for the interception of communications made to or from telecommunications devices that a person who is subject to a CSSO is using or is likely to use;
- Form 4G: This new form gives effect to proposed subparagraph 46A(2G)(g)(i) of the TIA Act by providing, as specified by the warrant, the authority for the interception of communications made to or from telecommunications services that a person who may be subject to Part 9.10 order (CSO) application is using or is likely to use;
- Form 4H: This new form gives effect to proposed subparagraph 46A(2G)(g)(ii) of the TIA Act by providing, as specified by the warrant, the authority for the interception of communications made to or from telecommunications devices that a person who may be subject to Part 9.10 order (CSO) is using or is likely to use;
- Form 5C: This new form gives effect to section 48 of the TIA Act in the circumstances mentioned in subsection 46(9) of the TIA Act by providing, as specified by the warrant, the authority for entry onto the premises specified by the warrant in order to install, maintain, use or recover equipment or a line used in the interception of communications being made to or from the telecommunications service specified by the warrant, and to intercept communications by the use of that equipment or line, with respect to an individual who is subject to a CSSO; and
- Form 5D: This new form gives to proposed section 48 in the circumstances mentioned in subsection 46(12) of the TIA Act by providing, as specified by the warrant, the authority for entry onto the premises specified by the warrant in order to install, maintain, use or recover equipment or a line used in the interception of

communications being made to or from the telecommunications service specified by the warrant, and to intercept communications by the use of that equipment or line, with respect to an individual who may be subject to a Part 9.10 order (CSO) application.

The proposed amendments would likely engage a number of human rights, and relevant safeguards are addressed in the Statement of Compatibility.

CONSULTATION

Consultation with relevant Commonwealth agencies was undertaken in relation to the Proposed Regulations, to the extent it was reasonably practicable in the time available.

POLICY IMPACT ANALYSIS

Given the proposed amendments are unlikely to have more than minor impact, a policy impact analysis was not required.

PART 1 – Preliminary

Section 1 – Criminal Code Regulations

Section 1 provides that the title of the instrument is the *Crimes Legislation Amendment (Community Safety Orders and Other Measures) Regulations 2023* (Proposed Regulation).

Section 2 – Commencement

This section would provide for the Proposed Regulations to commence on the day after the instrument is registered on the Federal Register of Legislation.

Section 3 – Authority

This section would provide that the Proposed Regulations is made under the *Criminal Code Act 1995* (the Code) and the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

Section 4 - Schedule(s)

This section would provide that each instrument that is specified in a Schedule to this instrument is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this instrument has effect according to its terms.

SCHEDULE 1 – Amendments

Criminal Code Regulations 2019

Item 1 – Paragraph 10(a)

Item 1 repeals wording within subparagraph 10(a) of the current the *Criminal Code Regulations 2019* (the Code Regulations) to remove the senior executive requirement of an AFP employee as a prescribed person. Paragraph 10 sets out the prescribed persons for the purposes of subsection 105A.19(1) of the Code (sharing information).

Senior executive employees of the Australian Federal Police (AFP) are listed as prescribed persons under the Code Regulations. The Code Regulations specify that information sharing must be at the senior executive level, which restricts the department's ability to only request or share information relating to eligible terrorist offenders with SES level AFP employees. This seniority restriction impedes the ability to share relevant operational information quickly and can lead to delays in obtaining information on an offender's current status whilst on a

PSO in the community. This impacts the ability of case managers to flag issues as they arise, leaving offenders on PSOs vulnerable to potential risks, or failure to address therapeutic needs in a timely manner.

The Proposed Regulations would remove the seniority requirement for AFP employees when requesting or sharing information under ss 105A.19(1) and (3) of the Code. This would allow any AFP employee to engage in the information sharing process and disclose information to the Attorney-General for the purpose of Division 105A of the Code.

In undertaking this function, the Attorney-General may obtain personal information. This information is given a significant level of protection under the Code and unauthorised disclosure of this information is an offence.

Item 2 – After Paragraph 10(d)

Paragraph 10 sets out the prescribed persons for the purposes of subsection 105A.19(1) of the Code. The Code Regulations only provide the states and territories the ability to request or share information from service providers, who provide support services connected with PSOs.

The Commonwealth is responsible for facilitating the therapeutic case management of Victorian terrorist offenders on PSOs, such as an extended supervision orders (ESO). Currently, the Code Regulations restrict the ability of the Commonwealth to directly request or share information with service providers, such as psychologists and support services. In addition, the *Privacy Act 1998* (Cth) (Privacy Act) provisions prevent the Attorney-General from requesting or sharing information with service providers which may contain personal information. This restricts the Attorney-General's ability to obtain relevant information for PSO considerations under Division 105A of the Code.

The Proposed Regulations would expand the list of prescribed persons to enable the Attorney-General (or their delegate) to directly request or share information with service providers, who provide services for or on behalf of the Commonwealth to eligible terrorist offenders under ss 105A.19(1) and (3) of the Code. This would support the department's monitoring of an eligible terrorist offenders' progress, development and rehabilitation while on a PSO.

Addressing this issue would allow stronger collaboration with the AFP on the ongoing case management of eligible terrorist offenders, enable case managers to address potential risks or

needs as they arise, and strengthen the department's advice to the Attorney-General regarding ESO conditions for eligible terrorist offenders.

In undertaking this function, the current information sharing provision is providing significant level of protection under the Code and unauthorised disclosure of this information is an offence.

Item 3 – Paragraph 10(g)

Paragraph 10 sets out the prescribed persons for the purposes of subsection 105A.19(1) of the Code. This include the Director- General of the Australian Security Intelligence Organisation, a Deputy Director- General of the Australian Security Intelligence Organisation, an ASIO employee or an ASIO affiliate (all within the meaning of the *Australian Security Intelligence Organisation Act 1979*).

The Proposed Regulations would make a minor technical amendment to the Code Regulations to update the reference to the 'Director-General Australian Security Intelligence Organisation' and 'Deputy Director-General of the Australian Security Intelligence Organisation' to 'the Director-General of Security' and 'Deputy-General of Security'.

Item 4 – At the end of Paragraph 10(h)

Paragraph 10 sets out the prescribed persons for the purposes of subsection 105A.19(1) of the Code.

Currently, the *Australian Passports Act 2005* (Cth) (the Passports Act) is not included in the Code Regulations; therefore, the department is unable to request information regarding passport cancellations and passport application rejections for relevant eligible terrorist offenders. This information may be relevant to an offender's risk and the ESO conditions needed to manage it. Currently, the Department of Foreign Affairs and Trade (DFAT) is responsible for administering the Passports Act and is not listed as a prescribed person in the Code Regulations. In addition, the Privacy Act provisions also prevent the Attorney-General from requesting or sharing information with DFAT, which may contain personal information. This restricts the Attorney-General's ability to obtain relevant information for PSO considerations under Division 105A of the Code.

The Proposed Regulations would introduce an additional prescribed person under the Code Regulations to enable the Attorney-General to request and share information with any employee of the Department who administers the Passports Act for the purpose of

Division 105A. This would ensure that the Attorney-General has all relevant passport information to assist the consideration of a PSO.

In undertaking this function, the current information sharing provision is provided a significant level of protection under the Code and unauthorised disclosure of this information is an offence.

Item 5 – At the end of Part 3 – Section 20A

This section would provide a Supreme Court of a State or Territory with guidance as to what matters it may consider when deciding if circumstances are beyond a serious offender's control for the purposes of paragraph 395.34(3)(a) of the Code. It is ultimately up to the Court as to what matters it considers, and what weight it gives to each matter.

Paragraph 20A(a) would provide that the Court may take into account the offender's financial circumstances. The offender's financial circumstances would be highly relevant in determining whether that offender is able to afford the costs of legal representation.

Paragraph 20A(b) would provide that the Court may take into account whether the offender has engaged in unreasonable conduct during the proceeding which has resulted in the offender being unable to afford any or all of the costs and expenses of legal representation. This matter may be relevant where, for example, a person is no longer able to afford legal representation as a result of unreasonably delaying the proceedings and knowingly incurring high legal costs.

Paragraph 20A(c) would provide that the Court may consider whether the offender has made efforts to obtain legal aid or legal assistance, and the outcomes of those efforts. Where the offender believes that he or she cannot afford the costs of legal representation for a CSO proceeding, the offender should make efforts to apply for legal aid or legal assistance. The outcomes of those efforts may also be relevant to the Court's decision. For example, the offender may not be granted access to legal aid if they can afford legal representation using funds available to them.

Paragraph 20A(d) would provide that the Court may also consider any other matter it considers relevant. The inclusion of this paragraph clarifies that matters in section 20A are not exhaustive, and do not prevent the Court from considering additional matters that it considers relevant.

It is anticipated that, as a civil proceeding, existing State and Territory Supreme Court processes would be applied and relied on to assess these costs.

Item 5 – At the end of Part 3 – Section 20B

This section would prescribe a list of persons for the purposes of subsections 395.44(1) and (4) of the Code. Subsections 395.44(1) and (4) of the Code provide that the Minister administering the *Migration Act 1958*, may request information from, and disclose information to, persons prescribed by the regulations to facilitate the execution of Division 395.

Division 395 of the Code contains the Commonwealth’s CSO Regime for non-citizens who have no real prospect of being removed from Australia in the reasonably foreseeable future and pose an unacceptable risk to the community. This Division of the Code allows the Immigration Minister to apply to the Supreme Court of a State or Territory for a CSO, which includes a community safety detention order (CSDO) and a community safety supervision order (CSSO).

Section 20B would prescribe a list of persons who:

- the Immigration Minister may request information from, being information that the Immigration Minister reasonably believes to be relevant to the administration or execution of Division 395 of the Code, and
- the Immigration Minister may disclose information to, if:
 - the information was acquired by the Immigration Minister, a legal representative of the Immigration Minister, the Secretary of the Department, or an Australian Public Service (APS) employee in the Department, and
 - the Immigration Minister reasonably believes that the disclosure is necessary to enable the person to exercise the person’s powers, or to perform the person’s functions or duties.

This section is designed to ensure all relevant agencies are able to share information where it relates to a serious offender eligible for a CSO. This information would support recommendations to the Immigration Minister on whether to apply for a CSO under Division 395 of the Code.

Persons that would be prescribed under section 20B for the purposes of facilitating the execution of Division 395 include:

- an Australian Federal Police employee
- certain members of State or Territory police forces
- persons employed by a State or Territory, or an authority thereof, whose duties relate to corrective services, justice or parole
- persons providing services for or on behalf of a State or Territory, or an authority thereof, in relation to corrective services, justice or parole
- persons who provide services for, or behalf of, the Commonwealth in relation to offenders who have a community safety order in force, or offenders whom the Immigration Minister is considering making application for such an order in relation to
- the Director of Public Prosecutions and the staff of their Office, and State and Territory equivalents
- the Director-General, a Deputy Director-General, and employees or affiliates of the Australian Security Intelligence Organisation
- an APS employee of a Department administered by the Minister administering the *Migration Act 1958* and *Australian Passports Act 2005*
- authorised officers within the meaning of Division 9A of Part IB of the *Crimes Act 1914* (Crimes Act) or persons who are performing functions under that Division under a delegation from such an authorised officer. Division 9A relates to the sharing of information relevant to federal offenders, and allows for information to be shared in the administration or execution of the sentencing, imprisonment and release of federal offenders
- a relevant expert who is appointed by the Immigration Minister under section 395.43 of Code or otherwise engaged by or on behalf of the Immigration Minister to assess the risk of a serious offender committing a serious violent or sexual offence for the purposes of the Division and
- a person who is engaged as a consultant or contractor, or is engaged or employed by such a person, to perform services for the Department administered by the Minister administering the *Migration Act 1958*. This ensures that information can be shared with and requested from service providers who manage and deliver immigration related programs and operations on behalf of the Commonwealth

Information held by police, public prosecution authorities, corrective services, intelligence agencies, and immigration authorities is crucial to facilitating the effective execution and administration of Division 395.

Section 20B extends the current list of prescribed persons in section 10 of the Code Regulations to additionally capture APS employees, contractors and consultants in immigration and border protection related functions.

This ensures the information sharing regime under subsections 395.44(1) and (4) of the Code is fit for purpose, and that information can be collected about a serious offender in relation to their engagement with the immigration and border protection environment, such as immigration detention. It is intended that the provision would capture Australian Border Force officials, and contractors and consultants, who manage and operate detention centres, as these persons hold information that could be useful for the administration and execution of the Division.

Item 6 – After paragraph 8(bc)

Item 6 inserts into section 8 of the TIA Regulations new paragraph 8(bd), 8(be) and (bf). This proposed amendment prescribes three new forms for authorising agencies to intercept communications made to or from the telecommunication service for the purposes of subsection 49(1) of the TIA Act.

The three forms are:

- Form 2D in Schedule 1 (paragraph 8(bd) of section 8 of the TIA Regulations);
- Form 2E in Schedule 1 (paragraph 8(be) of section 8 of the TIA Regulations); and
- Form 2F in Schedule 1 (paragraph 8(bf) of section 8 of the TIA Regulations).

The effect of this proposed amendment is to specify the forms for warrants issued under subsection 46(9) of the TIA Act, to which either subparagraph 46(9)(d)(i) or 46(2C)(d)(ii) of the TIA Act relate and subsection 46(12) of the TIA Act. See Item 9 for more information on Forms 2D, 2E and 2F.

Item 7 – After paragraph 8(fb)

Item 7 inserts paragraphs 8(fc), (fd), (fe) and (ff) into section 8 of the TIA Regulations. This proposed amendment prescribes new forms for authorising agencies to intercept telecommunications for the purposes of subsection 49(1) of the TIA Act.

The two new forms are:

- Form 4E in Schedule 1 (paragraph 8(fc) of section 8 of the TIA Regulations);
- Form 4F in Schedule 1 (paragraph 8(fd) of section 8 of the TIA Regulations);
- Form 4G in Schedule 1 (paragraph 8(fe) of section 8 of the TIA Regulations); and
- Form 4H in Schedule 1 (paragraph 8(ff) of section 8 of the TIA Regulations).

The effect of this proposed amendment is to specify the forms for warrants issued under:

- subsection 46A(2E) of the TIA Act, to which either subparagraph 46A(2E)(e)(i) or 46A(2E)(e)(ii) of the TIA Act relate, and
- subsection 46A(2G) of the TIA Act, to which either subparagraph 46A(2G)(g)(i) and 46A(2G)(g)(ii) relate.

See Item 10 for more information on Forms 4E, 4F, 4G and 4H.

Item 8 – At the end of Section 8

Item 8 inserts paragraph 8(j) and 8(k) into section 8 of the TIA Regulations. This proposed amendment prescribes two new forms for authorising agencies to intercept telecommunications for the purposes of subsection 49(1) of the TIA Act.

The two new forms are:

- Form 5C in Schedule 1 (paragraph 8(j) of section 8 of the TIA Regulations); and
- Form 5D in Schedule 1 (paragraph 8(k) of section 8 of the TIA Regulations).

The effect of this proposed amendment is to specify the form of warrant issued under section 48 in circumstances mentioned in subsection 46(9) and 46(12) of the TIA Act. See Item 11 for more information on Form 5C and 5D.

Item 9 – Forms 2D to 2F

Item 9 of the Proposed Regulations establishes new Forms 2D, 2E and 2F.

Forms 2D applies where a telecommunication service warrant for a CSSO is in force in relation to a particular person and is for the purpose of protecting the community from serious harm by addressing the unacceptable risk of a serious offender committing serious violent or sexual offences or determining whether the CSSO is being complied with.

Form 2F applies where a telecommunication service warrant for a CSSO is in force in relation to another person is for the purpose of protecting the community from serious harm by addressing the unacceptable risk of a serious offender committing serious violent or sexual offences or determining whether the CSSO is being complied with.

Form 2F ensures law enforcement have the authority to intercept communications that would provide contemporary evidence to assist in understanding a serious offender's level of risk, which would inform the decision of whether or not to apply for a Part 9.10 order application in relation to that offender.

Form 2D – Telecommunications service warrant for a community safety supervision order

This form is to be used by an eligible Judge or nominated AAT member, within the meaning of the TIA Act, acting under subsection 46(9) of that Act to which subparagraph 46(9)(d)(i) of the Act applies, to authorise the interception of communications made to or from a telecommunications service as specified by the warrant with respect to an individual who is subject to a CSSO (within the meaning of section 6UA of the Act).

Subsection 49(1) of the TIA Act provides that a warrant shall be in accordance with the prescribed form. Section 8 of the TIA Regulations provides that a warrant issued by an issuing authority under subsection 46(9)(d)(i) of the TIA Act shall be in accordance with Form 2D in Schedule 1 to the TIA Regulations.

Subsection 46(9) of the TIA Act sets out the circumstances in which a Part 9.10 warrant agency may apply for a CSSO warrant. Paragraph 46(9)(e) of the TIA Act provides:

“(e) information that would be likely to be obtained by intercepting under a warrant communications made to or from the service would be likely to substantially assist in connection with:

- (i) achieving a Part 9.10 object; or
- (ii) determining whether the community safety supervision order, or any succeeding community safety supervision order, has been, or is being, complied with; and”

Form 2E – Telecommunications service warrant for community safety supervision order— B-party

This form is to be used by an eligible Judge or nominated AAT member, within the meaning of the TIA Act, acting under subsection 46(9) of that Act to which subparagraph 46(9)(d)(ii)

of that Act applies. The eligible Judge or nominated AAT member may use the form to authorise the interception of communications made to or from a telecommunications service as specified by the warrant where a CSSO is in force in relation to another person (within the meaning of section 6UA of the Act), and the particular person is likely to communicate with the other person using the service.

Subsection 49(1) of the TIA Act provides that a warrant shall be in accordance with the prescribed form. Section 8 of the TIA Regulations provides that a warrant issued by an issuing authority under subsection 46(9)(d)(ii) of the TIA Act shall be in accordance with Form 2E in Schedule 1 to the TIA Regulations.

Subsection 46(9) of the TIA Act sets out the circumstances in which a Part 9.10 warrant agency may apply for a CSSO warrant. Paragraph 46(9)(e) of the TIA Act provides:

“(e) information that would be likely to be obtained by intercepting under a warrant communications made to or from the service would be likely to substantially assist in connection with:

- (i) achieving a Part 9.10 object; or
- (ii) determining whether the community safety supervision order, or any succeeding community safety supervision order, has been, or is being, complied with; and”

Form 2F – Telecommunications service warrant for Part 9.10 order application

This form is to be used by an eligible Judge or nominated AAT member, within the meaning of the TIA Act, under subsection 46(12) of that Act, to authorise the interception of communications made to or from a telecommunications service as specified by the warrant with respect to an individual who may be subject to a Part 9.10 order application.

Subsection 49(1) of the TIA Act provides that a warrant shall be in accordance with the prescribed form. Section 8 of the TIA Regulations provides that a warrant issued by an issuing authority under subsection 46(12) of the TIA Act shall be in accordance with Form 2F in Schedule 1 to the TIA Regulations.

Subsection 46(12) of the TIA Act sets out the circumstances in which a Part 9.10 warrant agency may apply for a warrant. Subsection 46(12) of the TIA Act provides the matters to which the Judge or nominated AAT member must have regard to when exercising their discretion to issue such a warrant.

The intention of this proposed amendment is to ensure law enforcement have the power to intercept communications that would provide contemporary evidence to assist in understanding an offender's level of risk, which would inform the decision of whether or not to apply for a Part 9.10 order application in relation to that offender.

Item 10 – Forms 4E, 4F, 4G and 4H in Schedule 1

Item 10 establishes new Forms 4E, 4F, 4G and 4H in Schedule 1 of the TIA Regulations.

Form 4E applies where a named person warrant for a CSSO is in force in respect of a person and is for the purpose of protecting the community from serious harm by addressing the unacceptable risk of a serious offender committing serious violent or sexual offences or determining whether the CSSO is being complied with.

Form 4F applies where a named person warrant for a CSSO is in force in respect of a person and is for the purpose of protecting the community from serious harm by addressing the unacceptable risk of a serious offender committing serious violent or sexual offences or determining whether the CSSO is being complied with.

Form 4G ensures law enforcement have the authority to intercept communications that would provide contemporary evidence to assist in understanding an offender's level of risk, which would inform the decision of whether or not to apply for a 9.10 order in relation to that offender's telecommunication services.

Form 4H ensures law enforcement have the authority to intercept communications that would provide contemporary evidence to assist in understanding an offender's level of risk, which would inform the decision of whether or not to apply for a 9.10 order in relation to that offender's telecommunication devices.

Form 4E – Named person warrant for community safety supervision order — telecommunications services

This form is to be used by an eligible Judge or nominated AAT member, within the meaning of the TIA Act, acting under subsection 46A(2E) of that Act to which subparagraph 46A(2E)(e)(i) of the Act applies, to authorise interceptions of communications made to or from any telecommunications service that a named person who is subject to a CSSO (within the meaning of section 6UA of the TIA Act) is using, or is likely to use.

Subsection 49(1) of the TIA Act provides that a warrant shall be in accordance with the prescribed form. Section 8 of the TIA Regulations provides that a warrant issued by an issuing authority under subsection 46A(2E) of the TIA Act to which subparagraph 46A(2E)(e)(i) of the TIA Act applies, shall be in accordance with Form 4E in Schedule 1 to the TIA Regulations.

Subsection 46A(2E) of the TIA Act sets out the circumstances in which a Part 9.10 warrant agency may apply for a named person warrant for a CSSO for the purposes of:

“(iii) achieving a Part 9.10 object; or

(iv) determining whether the community safety supervision order, or any succeeding community safety supervision order, has been, or is being, complied with; and”

Form 4F – Named person warrant for community safety supervision order—
telecommunications services

This form is to be used by an eligible Judge or nominated AAT member, within the meaning of the TIA Act, acting under subsection 46A(2E) of that Act to which subparagraph 46A(2E)(e)(ii) of the Act applies, to authorise interceptions of communications made by means of a particular telecommunications device or particular communication devices that a named person who is subject to CSSO (within the meaning of section 6UA of the TIA Act) is using, or is likely to use.

Subsection 49(1) of the TIA Act provides that a warrant shall be in accordance with the prescribed form. Section 8 of the TIA Regulations provides that a warrant issued by an issuing authority under subsection 46A(2E) of the TIA Act to which subparagraph 46A(2E)(e)(ii) of the TIA Act applies, shall be in accordance with Form 4F in Schedule 1 to the TIA Regulations.

Subsection 46A(2E) of the TIA Act sets out the circumstances in which a Part 9.10 warrant agency may apply for a named person warrant for a CSSO for the purposes of:

“(iii) achieving a Part 9.10 object; or

(iv) determining whether the community safety supervision order, or any succeeding community safety supervision order, has been, or is being, complied with; and”

Form 4G – Named person warrant for Part 9.10 order application—telecommunications services

This form is to be used by an eligible Judge or nominated AAT member, within the meaning of the TIA Act, acting under subsection 46A(2G) of that Act to which subparagraph 46A(2G)(g)(i) of the Act applies, to authorise interceptions of communications made to or from any telecommunications service that a named person who may be subject to a Part 9.10 order application is using, or is likely to use.

Subsection 49(1) of the TIA Act provides that a warrant shall be in accordance with the prescribed form. Section 8 of the TIA Regulations provides that a warrant issued by an issuing authority under subsection 46A(2G) of the TIA Act to which subparagraph 46A(2G)(g)(i) of the TIA Act applies, shall be in accordance with Form 4G in Schedule 1 to the TIA Regulations.

Subsection 46A(2G) of the TIA Act sets out the matters to which the Judge or nominated AAT member must have regard when determining to issue such a Part 9.10 order application.

Form 4H– Named person warrant for Part 9.10 order application—telecommunications devices

This form is to be used by an eligible Judge or nominated AAT member, within the meaning of the TIA Act, acting under subsection 46A(2G) of that Act to which subparagraph 46A(2G)(g)(ii) of the Act applies, to authorise interceptions of communications made by means of a particular telecommunications device or particular telecommunications devices that a named person who may be subject to a Part 9.10 order application is using, or is likely to use.

Subsection 49(1) of the TIA Act provides that a warrant shall be in accordance with the prescribed form. Section 8 of the TIA Regulations provides that a warrant issued by an issuing authority under subsection 46A(2G) of the TIA Act to which subparagraph 46A(2G)(g)(ii) of the TIA Act applies, shall be in accordance with Form 4H in Schedule 1 to the TIA Regulations.

Subsection 46A(2G) of the TIA Act sets out the matters to which the Judge or nominated AAT member must have regard when determining to issue such a Part 9.10 order application.

Item 11 – Form 5C and 5D in Schedule 1

Item 11 establishes new Form 5C and Form 5D. The new forms ensure law enforcement have the authority to install, maintain, use or recover equipment or a line, and intercept communications, that would provide contemporary evidence to assist in understanding an offender’s level of risk, which would inform the decision of whether or not to apply for a CSSO or a Part 9.10 order application in relation to that offender.

Form 5C – Warrant for entry onto premises and interception of communications for community safety supervision orders

Form 5C is to be used by an eligible Judge or nominated AAT member, within the meaning of the TIA Act, acting under section 48 of that TIA Act, to authorise entry onto premises where an agency was also able to apply for a warrant under subsection 46(9) of the Act, which authorises interceptions of communications to or from a service.

Subsection 49(1) of the TIA Act provides that a warrant shall be in accordance with the prescribed form. Section 8 of the TIA Regulations provides that a warrant issued by an issuing authority under section 48 of the TIA Act in relation to subsection 46(9) shall be in accordance with Form 5C in Schedule 1.

Where applicable, section 48 of the TIA Act sets out the circumstances in which a Part 9.10 warrant agency may apply for a warrant for entry onto premises and interception of communications for CSSO.

Form 5D – Warrant for entry onto premises and interception of communications for Part 9.10 order applications

This form is to be used by an eligible Judge or nominated AAT member, within the meaning of the TIA Act, acting under section 48 of that Act, to authorise entry onto premises to install, maintain, use or recover equipment or a line, and intercept communications, where an agency was also able to apply for a warrant under subsection 46(12) of the Act, which authorises interceptions of communications to or from a service.

Subsection 49(1) of the TIA Act provides that a warrant shall be in accordance with the prescribed form. Section 8 of the TIA Regulations provides that a warrant issued by an issuing authority under section 48 of the TIA Act in relation to subsection 46(12) shall be in accordance with Form 5D in Schedule 1.

Subsection 46(12) of the TIA Act sets out the matters to which the Judge or nominated AAT member must have regard when determining whether to issue a warrant for a Part 9.10 order application.

Where applicable, section 48 of the TIA Act sets out the circumstances in which a Part 9.10 warrant agency may apply for a warrant for entry onto premises and interception of communication for Part 9.10 order applications.

Statement of Compatibility with Human Rights

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

Crimes Legislation Amendment (Community Safety Orders and Other Measures) Regulations 2023

This Disallowable Legislative Instrument 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 Disallowable Legislative Instrument

The *Crimes Legislation Amendment (Community Safety Orders and Other Measures) Regulations 2023* (Proposed Regulation) would facilitate information-sharing for the purpose of Division 105A of the *Criminal Code Act 1995* (the Code) and support the implementation of the Community Safety Orders (CSOs) regime under Division 395 of the Code introduced by the *Migration and Other Legislation Amendment (Bridging Visas, Serious Offenders and Other Measures) Act 2023* in response to the High Court of Australia's judgment in *NZYQ v Minister for Immigration, Citizenship and Multicultural Affairs* [2023] HCA 37.

The Proposed Regulations would amend the:

- (a) *Criminal Code Regulations 2019* (the Code Regulations)
- (b) *Telecommunications (Interception and Access) Regulations 2017* (the TIA Regulations).

The Code Regulations are made under the Code. Part 2 of the Code Regulations relates to the security of the Commonwealth and provides for control orders, preventative detention, and post-sentence orders (PSOs) in relation to terrorism offences committed by eligible terrorist offenders. Part 3 of the Code Regulations relates to matters relating to dangers to the community.

Section 5 of the Code provides that the Governor-General may make regulations prescribing matters, required or permitted by the Code to be prescribed, or necessary or convenient to be prescribed for carrying out or giving effect to the Code.

The *Telecommunications (Interception and Access) Act 1979* (TIA Act) protects the privacy of, and regulates access to, the content of telecommunications and telecommunications data. Section 300 of the TIA Act provides that the Governor-General may make regulations, not inconsistent with the Act, 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.

Amendments to the Code Regulations

The Proposed Regulations would prescribe matters that a Supreme Court of a State or Territory may take into account in determining whether circumstances are beyond a serious offender's control in relation to engaging a legal representative in CSO proceedings under Division 395 of the Code, and prescribe a list of persons that the Immigration Minister, as the Minister administering the Migration Act 1958, may request information from, and disclose information to, to facilitate the execution of Division 395 of the Code.

The Proposed Regulations would also enhance information-sharing processes for the purposes of Division 105A of the Code.

The human rights implications of each schedule contained in the instrument have been dealt with below.

Amendments to the TIA Regulations

The Proposed Regulations amend the TIA Regulations as a consequence of passage of the *Migration and Other Legislation Amendment (Bridging Visas, Serious Offenders and Other Measures) Act 2023*. Specifically, the Proposed Regulations would extend the application of telecommunications service warrant, named person warrant and warrant for entry on premise and interception of communications forms to be available in relation to Community Safety Supervision Orders (CSSOs) and Part 9.10 order applications.

These proposed amendments ensure the current warrant forms are amended to capture the new provisions and orders inserted into the TIA Act by the *Migration and Other Legislation Amendment (Bridging Visas, Serious Offenders and Other Measures) Act 2023*.

Human rights implications

This Disallowable Legislative Instrument engages the following rights:

- the right to a fair trial and fair hearing, and minimum guarantees in criminal proceedings under Article 14 *International Covenant on Civil and Political Rights* (ICCPR),
- the right to privacy in Article 17 of the ICCPR,
- the right to freedom of opinion and expression in Article 19 of the ICCPR.

The right to a fair trial and fair hearing, and minimum guarantees in criminal proceedings

Article 14(1) of the ICCPR relevantly provides that:

All persons shall be equal before the courts and tribunals. In the determination of any criminal charge against him, or of his rights and obligations in a suit at law, everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law.

Article 14(3) of the ICCPR provides that:

In the determination of any criminal charge against him, everyone shall be entitled to the following minimum guarantees, in full equality:

...

(d) To be tried in his presence, and to defend himself in person or through legal assistance of his own choosing; to be informed, if he does not have legal assistance, of this right; and to have legal assistance assigned to him, in any case where the interests of justice so require, and without payment by him in any such case if he does not have sufficient means to pay for it.

The Instrument engages and promotes the right to a fair trial and a fair hearing, the right to minimum guarantees in criminal proceedings and in a suit at law in article 14 of the ICCPR.

Proposed Regulations 20A – Offender unable to engage legal representative in proceedings – Matters court may take into account in determining whether circumstances beyond offender’s control

Proposed Regulations 20A refers to paragraph 395.34(3)(a) of the Criminal Code.

Subsection 395.34 of the Criminal Code applies to proceedings for a CSSO or a CSDO where

the offender, due to circumstances beyond his or her control, is unable to engage a legal representative.

Under paragraph 395.34(2), the Supreme Court of a State or Territory may make an order to stay the proceeding, and/or require the Commonwealth to bear all or part of the reasonable costs and expenses of the offender's legal representation for the proceeding.

Paragraph 395.34(3) provides that the Code Regulations may prescribe matters that the Court may, must or must not take into account in determining whether circumstances are beyond the offender's control.

Proposed Regulations 20A provides guidance to the Court in making an order under section 395.34(2) of the Code. In particular, it prescribes matters the Court may take into account in determining whether circumstances are beyond an offender's control. The matters prescribed by the Proposed Regulations 20A seek to ensure the Court has considered key issues in determining the appropriateness of making the order. Paragraph 20A(d) expressly provides that it does not limit the ability of the Court to consider additional matters to those prescribed.

Examples of the types of matters that a Court may take into account in determining whether circumstances are beyond an offender's control include the offender's financial circumstances, and whether the offender has engaged in unreasonable conduct during the proceeding that has contributed to their inability to afford any or all of the costs and expenses of obtaining legal representation for the proceeding.

By ensuring, where appropriate, the offender has the benefit of legal representation, the Proposed Regulations promote the offender's right to a fair trial and fair hearing, as well as the right to minimum guarantees as discussed above and as expressed in article 14 of the ICCPR.

Protection against unlawful and arbitrary interference with privacy

Article 17 of the ICCPR provides:

No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

Pursuant to Article 17(1) of the ICCPR, any interference with an individual's privacy must have a lawful basis. In addition to requiring a lawful basis for limitation on the right to privacy, Article 17 prohibits arbitrary interference with privacy. Interference which is lawful

may nonetheless be arbitrary where that interference is not in accordance with the objectives of the ICCPR and is not reasonable, necessary and proportionate in the circumstances.

Proposed Regulations 10 – Sharing of information

This Instrument engages the right to privacy by allowing disclosure of information held by the relevant department and/or prescribed persons. These persons may include psychologists, counsellors or relevant service providers who may assist in the case management under a PSO or a CSO. These department and/or prescribed persons may be provided personal information about the eligible offender, relevant to the services being provided while on an order.

Information may include updates from services providers on the progress of an eligible offender on an order, including psychology reports or assessment notes by specialist service providers. As noted above, the disclosure of personal information without a person's consent would engage, and limit, the protection from arbitrary and unlawful interference with privacy in article 17 of the ICCPR.

The right in Article 17 may be subject to permissible limitations, where the limitations are authorised by law and are not arbitrary. In order for an interference with the right to privacy to be permissible, the interference must be authorised by law, be for a reason consistent with the ICCPR and be reasonable in the particular circumstances. The UN Human Rights Committee has interpreted the requirement of 'reasonableness' to imply that any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case

To the extent that the measures in the instrument would limit the right in Article 17 of the ICCPR, they are lawful and non-arbitrary.

The proposed amendments in the instrument would allow information to be requested and shared with the relevant department, which is limited to disclosures that are necessary to achieve this purpose. Disclosures may occur where a eligible offender has attended psychology sessions, and the psychologist (a prescribed persons) responds to a request for information from the relevant Minister, to assist in the consideration of a PSO or CSO review.

The objective of the information sharing provision is to ensure the protection of the community and eligible offenders, through efficient information sharing and early risk identification.

In the absence of the proposed amendments, a person not listed as a prescribed person who discloses information about an eligible offender to the relevant Minister may be unable to do so without breaching the Privacy Act.

Proposed Regulations 20B – Sharing information – prescribed persons

Proposed Regulations 20B interacts with the right to privacy by allowing, in limited circumstances, the Immigration Minister to share information with a prescribed list of persons.

Sharing information with a prescribed list of persons is a permissible limitation on the right to privacy. The Immigration Minister may request information from prescribed persons under Division 395.44 only where he or she reasonably believes that information to be relevant to the administration or execution of the Division. Further, the Immigration Minister may only disclose information to prescribed persons where he or she reasonably believes that the disclosure is necessary to enable the person to exercise their powers or perform their functions or duties.

Proposed Regulations 20B specifically limit the list of persons with whom information may be shared to ensure that information is only provided to or requested from those with a relevant function or purpose. Prescribed persons are also protected from breaching any law of the Commonwealth, a State or a Territory (whether written or unwritten), in providing information to the Immigration Minister under Sections 395.44(3) and (5) of the Code. In the absence of the proposed amendments, a person not listed as a prescribed person who discloses information about an offender in relation to the CSDO and CSSO scheme, may be unable to do so without breaching the Privacy Act.

Noting that the CSDO and CSSO scheme is necessary for protecting community safety, the proposed amendments in the instrument would facilitate information to be requested and shared with the Attorney-General and/or the Immigration Minister, which is limited to disclosures that are necessary to achieve this purpose.

This framework appropriately limits the unnecessary or further disclosure of information. To the extent that the measures in Proposed Regulation 20B limit the right in Article 17 of the ICCPR, they are lawful and not arbitrary.

Clause 9 to 11– TIA Regulations Forms

The purpose of Clause 9 to 11 of Schedule 1 of the Disallowable Legislative Instrument is to prescribe the forms for the issuing of warrants under sections 46, 46A and 48 of the TIA Act. The Disallowable Legislative Instrument gives effect to these provisions of the TIA Act by prescribing the relevant form for warrants for a CSSO or a Part 9.10 order application. To the extent that personal information is contained in the forms, the right to privacy would be engaged.

Requiring the inclusion of limited personal information in these forms is a permissible limitation on the right to privacy. The issuing of warrants under the TIA Act relating to the CSDO and CSSO scheme would assist in protecting the community from serious harm by addressing the unacceptable risk of a serious offender committing serious violent or sexual offences, determining whether a CSSO has been or is being complied with or determining whether an application for a Part 9.10 order under the TIA Act in relation to the offender should be made. In this regard, the proposed amendments pursue a legitimate objective.

This limitation is authorised by law and is not arbitrary, in that it is necessary, reasonable and proportionate to the legitimate objective pursued. The personal information to be included in the forms is limited to certain types of identifying information necessary to ensure the warrant is applied to the intended target, such as a person's name and the person's date of birth. The inclusion of this limited identifying information also promotes the privacy of other individuals by ensuring the warrant is not mistakenly applied to persons who are not the intended target of the warrant. The information included in the form is not subject to publication, and would be issued and used by an eligible Judge or nominated AAT member for the limited purpose of issuing a warrant under sections 46, 46A and 48 of the TIA Act.

Protection of freedom of opinion and expression

Article 19 of the ICCPR provides that:

Everyone shall have the right to hold opinions without interference. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. The exercise of the rights provided for in paragraph 2 of this article carries

with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

- a. For respect of the rights or reputations of others;*
- b. For the protection of national security or of public order (order public), or of public health or morals.*

This instrument engages this right by allowing to access information in relation to eligible offenders.

Article 19 may be subject to permissible limitations, where the limitations are authorised by law and are not arbitrary. In order for an interference to the right to access information be permissible, the interference must be authorised by law, be for a reason consistent with the ICCPR and be reasonable in the particular circumstances. The UN Human Rights Committee has interpreted the requirement of ‘reasonableness’ to imply that any interference to the right to access information must be proportional to the end sought and be necessary in the circumstances of any given case.

To the extent that the measures in the instrument would limit the right in Article 19 of the ICCPR, they are lawful and non-arbitrary.

By engaging information-sharing provisions, this may limit the offender’s right to access information disclosed between the relevant department and prescribed persons. Eligible offenders are informed and provided copies of material that would be relied upon if a PSO or CSO application (or review) is made in Court, due to specific disclosure obligations under the Code. Given the sensitive nature of the material obtained by intelligence and enforcement agencies, this information may be subject to information protection mechanisms such as Public Interest Immunity (PII) or secrecy claims, which may limit an offender’s right to access information. This is for the legitimate purpose of the protection of Australia’s national security and the community.

Prescribed persons are protected from breaching any law of the Commonwealth, a State or a Territory (whether written or unwritten), in providing information to the relevant Minister under the Code. The proposed amendments in the instrument would allow information to be requested and shared with the relevant department, and is limited to disclosures that are necessary to achieve this purpose.

The objective of the information sharing provision with listed prescribed persons is to ensure the protection of the community and eligible offenders, through efficient information sharing and information protection.

Safeguards relevant to the protection of the right to access information include disclosure and non-disclosure obligations under the Code require the applicant to provide the offender a copy of the application for a CSO or PSO (or a CSO or PSO review).

In the absence of the proposed amendments, a person who discloses information to a person not prescribed under the proposed Regulations may be unable to do so without breaching the Privacy Act.

Conclusion

The Disallowable Legislative Instrument is compatible with human rights because to the extent that it may limit human rights, those limitations are reasonable, necessary and proportionate to achieve the legitimate objective of the protection of Australia's national security and the community.