THE HON PETER DUTTON MP
MINISTER FOR HOME AFFAIRS

Ref No: MS20-000874

Senator Helen Polley
Chair
Senate Scrutiny of Bills Committee
Suite 1.111
Parliament House
CANBERRA ACT 2600

Dear Senator Polley

Thank you for your letter dated 20 April 2020 requesting further information on the Telecommunications Legislation Amendment (International Production Orders) Bill 2020.

My response for the Committee's consideration is enclosed.

Yours sincerely

18/05/20

PETER DUTTON

Telecommunications Legislation Amendment (International Production Orders) Bill 2020

Trespass on personal rights and liberties—international production orders

1.92 The committee requests the minister's advice regarding why it is necessary and appropriate to allow IPOs to be issued by members of the AAT.

The Bill provides for a range of independent decision-makers to authorise international production orders for disclosure of intercepted communications, stored communications and telecommunications data. To assist the Committee, a table setting out which decision-makers are able to authorise different types of orders under the Bill and the TIA Act currently is set out at **Annexure A**.

Administrative Appeals Tribunal (AAT) members, judges, magistrates, and the Attorney-General, all play a critical role as independent decision-makers in authorising investigatory powers domestically in the current regimes under the *Telecommunications (Interception and Access) Act 1979* (TIA Act). In accordance with this current domestic approach, the Bill recognises the value of having an independent decision-maker with the skillset of being a qualified legal practitioner given the complexity of the decision-making involved in authorising investigatory powers internationally and the inherent balancing of law enforcement or national security powers with affected individuals' privacy and other rights and liberties required.

The ability for nominated AAT members to authorise the use of investigatory powers is not new. For example, nominated AAT members have played an independent decision-maker role in investigatory powers legislation, including in relation to interception and stored communication warrants under the TIA Act since 1998. Nominated AAT members also issue surveillance device warrants and computer access warrants under the *Surveillance Devices Act 2004*. The skill and experience of AAT members make them ideal candidates to assess applications for international production orders and make independent decisions on their compliance with the legislative requirements. In addition, the framework and principles under which AAT members operate safeguard the functional independence of their decisions.

The skill, competence, and independence of AAT members makes them suitable to assess applications for international production orders and to make independent decisions in accordance with the legal requirements under the Bill. AAT members undertake this independent decision-maker role in their personal capacity. AAT members must consent to being made an independent decision-maker under specific regimes of the TIA Act (including the Bill) and the Attorney-General must nominate them. Providing a wide range of independent decision-makers (e.g. AAT members, judges and magistrates) ensures there is a sufficient pool of available decision-makers to authorise orders sought by agencies. This is particularly important given all law enforcement agencies across Australia utilise the TIA Act to obtain these kinds of investigatory powers.

In terms of international production orders that relate to national security, this will be limited to nominated AAT Security Division members only after the consent of the Attorney-General has been received. This ensures there is a rigorous process of independent scrutiny with ASIO being required to satisfy both the Attorney-General (as the First Law Officer with a longstanding role in approving ASIO's intelligence collection powers) and a nominated member of the AAT, that the legislative thresholds have been met before an international production order can be issued. The Inspector-

General of Intelligence and Security will also provide oversight of ASIO's use of powers under the legislation.

For the above reasons, the Government sees the utilisation of AAT members in their personal capacity as independent decision-makers as appropriate, necessary and critical to the effective operation of the TIA Act and the Bill.

1.96 The committee requests the minister's advice as to whether the bill could be amended to include a national public interest monitor scheme so that public interest monitors may make submissions in relation to all IPO applications.

In accordance with the current approach to domestic law enforcement interception warrants under the TIA Act, the Bill aligns international production orders for interception to ensure that, where Public Interest Monitors are available in relation to domestic interception warrants, they will also be available for interception international production orders.

At present, Public Interest Monitors only exists within Victoria and Queensland. Public Interest Monitors perform a broad oversight role over their jurisdiction's law enforcement agencies including when applying for certain types of warrants, such as interception warrants. Consistent with current practices, the Bill intentionally gave the ability to facilitate the role of the Public Interest Monitors for international production orders relating to interception.

Other Australian States and Territories have not legislated for this office within their jurisdictions. Consequently, the Bill only provides for the Public Interest Monitors in Victoria and Queensland. These Offices were established in Victoria under the *Public Interest Monitor Act 2011* (Vic), and various pieces of legislation in Queensland, including the *Police Powers and Responsibilities Act 2000* (Qld) and the *Crime and Corruption Act 2001* (Qld).

1.98 The committee requests the minister's advice as to whether the bill could be amended to require that, for all IPOs, the relevant decision maker must be satisfied that an IPO would be 'likely to substantially assist' with the relevant purpose for which the IPO is sought, rather than merely 'likely to assist'.

This Government considers that *'likely to assist'* is the appropriate threshold, as set out in the Bill. The threshold of *'likely to assist'* applies for all warrants under the TIA Act other than control order warrants. In terms of the Bill, this threshold applies to both intelligence and law enforcement agencies for international production orders to authorise intercept live communications as well as for stored communications and telecommunications data. When applying for any of these international production orders, agencies are required to demonstrate that the use of the warrant would be likely to assist in connection with those purposes.

The issuing authority must be satisfied that the information to be gathered would be *'likely to assist'* in meeting the purpose of the warrant. This criterion is then balanced alongside a range of other factors decision-makers must take into account, such as having regard to privacy interference and the gravity of conduct (for law enforcement warrants).

Replacing the threshold of *'likely to assist'* with the threshold of *'likely to substantially assist'* may have the effect of preventing law enforcement and intelligence agencies from accessing overseas information likely to assist in the investigation of serious crime or matters relating to national security. During the early stages of an investigation, it would be extremely difficult for agencies to demonstrate in advance of reviewing the information that the information will be *'likely to substantially assist'* the investigation. For example, telecommunications data, such as account details

and IP addresses, are often collected during the early stages of an investigation. When seeking an order, agencies need to demonstrate that this information is likely to assist the investigation, for example by determining a link between an account and the suspected criminal activity or offender and thereby identifying further lines of inquiry.

One of the policy objectives of this legislation is the recognition that the digital communications landscape has changed dramatically in the last decade, with communications technology providing a plethora of communications options on any given device - from traditional telecommunications and SMS through to social media and encrypted communications applications - each provided by a separate communications provider and each requiring a separate international production order. In many cases it would not be possible to know ahead of receiving the information if the data provided by any given communications provider will be the information that would '*substantially assist*' an investigation. A higher threshold could therefore be detrimental to investigations by removing a critical line of inquiry during the early stages of an investigation.

For completeness, the Government notes that monitoring powers within the TIA Act that relate to control orders are subject to the threshold of *'substantially assist'*. The imposition of a higher threshold for monitoring powers is appropriate because control orders have a protective or preventative purpose by facilitating monitoring of the person's compliance with the requirements of the control order, and the person is not necessarily suspected of involvement in further criminal activity since the control order was imposed. Accordingly, the Government has applied the exact same thresholds to international production orders relating to control orders.

1.104 The committee requests the minister's advice regarding whether the 3 month period in subclause 81(1) of proposed Schedule 1 to the TIA Act could be reduced to provide the Ombudsman with more immediate oversight of the issuing of control order IPOs.

The inclusion of a three month period in subclause 81(1) of the Bill reflects advice from the Commonwealth Ombudsman that given this is a new scheme whose frequency of use is not yet known, a period of three months would be more appropriate to facilitate timely oversight. This is already a marked reduction from current regimes. Both the *Crimes Act 1914* and the TIA Act establish a six month notification period.

The Commonwealth Ombudsman conducts its inspections of agencies' use of covert and intrusive powers retrospectively, with records generally assessed after the relevant warrant, authorisation or order has ceased to be in force. As such, inspections of records regarding control order international production orders are likely to occur some months after the Commonwealth Ombudsman has been notified of a control order international production order being issued. However, it is likely to significantly assist the Commonwealth Ombudsman to schedule and allocate resources for inspections, especially as it is anticipated that the use of the international production order regime will likely increase compared to current levels.

1.105 The committee also requests the minister's advice as to whether clause 144 of proposed Schedule 1 to the TIA Act could be amended to provide that the Ombudsman has the power to obtain relevant information from officers and members of staff if the Ombudsman has 'reasonable grounds to *suspect*' that the officer or member of staff is able to give the relevant information, rather than the higher threshold of 'reasonable grounds to *believe*'.

Clause 144 was drafted to mirror the same oversight powers of the Commonwealth Ombudsman contained within section 87 of the TIA Act. This is also consistent with other Commonwealth legislation, such as the *Crimes Act 1914*. Accordingly, amending the '*reasonable grounds to believe*'

threshold to '*reasonable grounds to suspect*' threshold, would require broader consideration across not only the TIA Act, but other Commonwealth legislation. The Government views that amending only the TIA Act (or parts of the TIA Act) would lead to considerable confusion as to what thresholds apply under different pieces of legislation despite the oversight role of the Commonwealth Ombudsman being broadly consistent across Commonwealth legislation.

Delegation of administrative powers—applications for international production orders

1.109 The committee requests the minister's advice regarding why it is necessary and appropriate to allow a broad range of persons to make an application for an international production order.

The Bill allows for an appropriate range of Commonwealth, State and Territory agencies to make an application for an international production order. This is primarily to reduce the burden on the current mutual legal assistance regime through providing an alternative investigative pathway and to ensure that investigations of serious crime and national security, and the monitoring of control orders, are able to be undertaken in a timely and effective manner.

The agencies and people within those agencies that can make an application for an international production order is intended to mirror the current arrangements under the TIA Act. The same agencies who can access this information domestically can do so internationally, in order to ensure they can successfully investigate serious crime, national security matters, and monitor control orders. Chief Officers of relevant agencies can delegate their powers to appropriate persons within their agencies to streamline processes to assist the relevant agency to enact and discharge its functions. Law enforcement and national security officers will receive training on the legislative requirements for making applications and will be supported by their legal areas to ensure that applications are of a high quality, and meet legislative requirements.

In terms of limiting who within agencies can make an application, please see response to 1.110 below for response.

1.110 The committee also requests the minister's advice as to whether the bill could be amended to:

- **limit the persons who can make an application for an international production order to only the heads of relevant agencies and members of the senior executive service (or equivalent); or**
- **at a minimum, require that the relevant agency head be satisfied that persons authorised to apply for an IPO have the relevant qualifications and expertise to do so.**

Consistent with the TIA Act regime, the Bill gives certain officers within agencies the ability to delegate the power to apply for an international production order. Independent of this consistency with domestic regimes, the separate policy reasoning for this is two-fold. Firstly, given the potential high volume of international production orders from Australian agencies, requiring agency heads or members of the senior executive service to make each application for an international production order would significantly reduce the speed with which agencies can request data under the international production order scheme and thereby significantly impair its utility. Secondly, agencies will be best placed to determine which officers are sufficiently qualified and across the factual circumstances of the investigations to ensure that independent decision-makers have before them sufficient opportunities to query facts forming the foundation of the application. In many cases, this

may be the relevant investigating officer in charge of an investigation, rather than agency heads or members of the senior executive service.

Australia's law enforcement and national security agencies provide all officers with high levels of training and apply appropriate levels of oversight to officers when making warrant applications and authorisations through clearance chains and, in the case of law enforcement, the chain of command. Similar training and oversight will apply in respect of officers dealing with international production orders. Training often includes the legislative requirements for making applications, as well as outlining any support officers would receive from their respective legally qualified staff. This ensures that applications are of a high quality, and meet legislative requirements set by the Australian Parliament.

It is anticipated that before an agency may apply for an international production order under the Bill, the Australian Designated Authority will first examine the capabilities of the agency and offer training on the international production order framework to that agency's relevant personnel. If the Australian Designated Authority is satisfied of the agency's ability to comply with the requirements of the international production order regime, the Australian Designated Authority may certify that agency as eligible to seek communications data through the channels established by the Bill and the relevant designated international agreement. As part of that certification process, the agency will need to demonstrate that persons authorised to apply for an international production order are appropriately qualified.

While there is flexibility to determine who is best placed to make an application for each individual agency or department, other safeguards such as orders only being issued by an independent decision-maker (e.g. an eligible judge or nominated AAT member) stand as a guard for insufficient or poor applications. Comprehensive oversight arrangements by the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security will also create accountability for how agencies approach the application process. For the above reasons, the Government does not think it is necessary to limit who can apply for an international production order.

No-invalidity clause

1.114 The committee requests the minister's advice as to the rationale for including a no-invalidity clause in relation to requirements to notify the Ombudsman about the issuing of control order IPOs or where the chief officer of an agency has contravened paragraph 114(1)(d).

The notification requirement in clause 81 facilitates Commonwealth Ombudsman oversight of agency use of the international production order regime as it relates to control orders. This additional notification requirement in respect of control order international production orders is necessary given the extraordinary nature of the control order monitoring powers. Sub clause 81(3) seeks to clarify that if an agency fails to comply with the administrative requirements in sub clauses (1) or (2), the validity of the order remains unaffected. The purpose of this clause is to ensure that an administrative oversight does not result in the potential for invalidity.

Control order international production order agencies are required to comply with their reporting obligations in this clause and more broadly throughout the Bill. However, sub clause 81(3) ensures that where an administrative reporting obligation is included and contravened, the contravention would not undermine the validity of the order, which could result in perverse outcomes eventuating,

for instance the inability to obtain information relevant to preventing a terrorist attack or subsequent prosecution relating to that potential attack.

Control order international production order agencies will be subject to strict oversight by the Commonwealth Ombudsman, as is the case for existing agencies that can apply for a control order warrant. Failure to comply with obligations in clause 81 may result in the investigation and public reporting on agency practices. This is consistent with current practices under the TIA Act for domestic control order warrants.

Delegation of administrative powers—functions of the Ombudsman

1.117 The committee requests the minister's advice as to why it is necessary to allow most of the Ombudsman's powers and functions to be delegated to APS employees at any level.

The broad delegation power allows the Commonwealth Ombudsman to determine how best to allocate resources and who the most appropriate officers will be when executing the functions or powers of the Commonwealth Ombudsman. This position is consistent with existing powers to delegate under the TIA Act.

This provision, and the provision at clause 149 regarding immunity from suit, replicate long standing provisions contained in the *Ombudsman Act 1976* (subsections 33 and 34) and mirror similar provisions contained in the oversight and accountability regimes established in the *Telecommunications (Interception and Access) Act 1979* and the *Surveillance Devices Act 2004* (Part 6), and the *Crimes Act 1914* (Part IAB).

The purpose of the delegation provision is to ensure that the staff of the office of the Commonwealth Ombudsman can perform the functions of the Commonwealth Ombudsman as required. It is important that the Commonwealth Ombudsman be able to determine the most efficient, effective and appropriate means of operationalising his functions as between himself and his staff cognisant of the powers involved and the expertise required to exercise them. In practice exercise of these functions and powers is limited to members of the team within the office of the Commonwealth Ombudsman responsible for conducting inspections of covert and intrusive powers by agencies.

1.118 The committee also requests the minister's advice as to whether the bill could be amended to:

- **provide some legislative guidance as to the scope of powers that might be delegated, or the categories of people to whom those powers might be delegated; or**
- **at a minimum, require that the Ombudsman be satisfied that persons performing delegated functions and exercising delegated powers have the expertise appropriate to the function or power delegated.**

The choice of delegate is largely a matter to be determined by the person making the delegation. However, the Government expects that where delegation is appropriate and permitted by domestic law, the original decision-maker will consider the appropriateness and the expertise required to perform that delegation effectively and in line with Australian community expectations.

Immunity from liability

1.121 The committee requests the minister's advice as to why it is necessary to provide the Ombudsman, an inspecting officer, or a person acting under an inspecting officer's direction or authority with immunity so that affected persons have their right to bring an action to enforce their legal rights limited to situations where lack of good faith is shown.

As mentioned above, clause 149 ensures the Commonwealth Ombudsman and staff with the office of the Commonwealth Ombudsman are able to perform their inspection functions under Part 10 without being impeded by the possibility of legal action. This provision is fundamental to enabling the Commonwealth Ombudsman and their staff to carry out their functions and powers freely and independently within the confines of the law. This immunity only applies if the inspection functions are being carried out in good faith. Immunity provisions of this kind are long-standing safeguards afforded to the Commonwealth Ombudsman and staff of the office of the Commonwealth Ombudsman, and similar immunities are contained elsewhere, such as section 33 of the *Ombudsman Act 1976*.

Evidentiary certificates

1.125 The committee therefore requests the minister's advice regarding whether the bill can be amended to provide that an evidentiary certificate made under clause 161 will be prima facie evidence rather than conclusive evidence of the matters stated in the certificate.

Both prima facie and conclusive evidentiary certificates continue to be vital to the functioning of the TIA Act, and indeed, the effective administration of justice. Since the early 1990s, the TIA Act has included a framework for the use of evidentiary certificates. Consistent with existing provisions in the TIA Act, evidentiary certificates issued by designated communication providers are to be received into evidence in proceedings as conclusive evidence of the matters stated in the certificate, and evidentiary certificates issued by law enforcement are to be received into evidence in proceedings as prima facie evidence of the matters stated in the certificate.

The *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (the Guide) sets out best practice in terms of the application of whether evidentiary certificate provisions are prima facie or conclusive evidence of the matters stated within. The Guide also notes evidentiary certificate provisions may specify that certificates are conclusive evidence of the matters stated in it where they cover technical matters that are sufficiently removed from the main facts at issue.

As noted by the Committee, the evidentiary certificates under clause 161 are to be treated in proceedings as conclusive evidence of the matters stated within from foreign designated communications providers. The policy objective here is the recognition of the inherent difficulties associated with having to have persons from those providers attend court to give witness testimony on matters that are merely technical or formal matters the provider had undertaken to comply with the international production order. These difficulties are likely to be compounded by the expected numbers of international production orders that will be focused on a few large foreign designated communications providers.

These evidentiary certificates will not cover matters in dispute or matters that go to questions of legality. The provision of conclusive evidentiary certificates that apply to the technical or formal matters will ensure that courts have complete information before them to assist in the administration of justice.

Trespass on personal rights and liberties

Lack of parliamentary oversight

Privacy

1.131 Based on the above, the committee therefore considers that the provisions as currently drafted have the potential to significantly trespass on a person's rights and liberties, particularly in circumstances where access to information held in Australia may be given to foreign jurisdictions whose governance structures are not underpinned by respect for the rule of law and the separation of powers.

The Bill facilitates Australia entering into international cross-border access to data agreements with like-minded foreign governments who share Australia's commitment to combating serious crime, rule of law principles, and who strive for electronic surveillance laws that respect the balance between the needs of law enforcement and national security with protecting their communities from arbitrary and unlawful interference to their privacy. Whilst the Bill provides the mechanism for these agreements to be designated by regulation (clause 3), before getting to this point agreements will be subject to considerable parliamentary and public scrutiny, such as:

1. The Australian Government will conduct a thorough assessment of the privacy regime of the foreign country before entering into, and during, any agreement negotiations.
2. The Attorney-General and the Minister for Foreign Affairs will approve any proposed agreement before it is signed. Both Ministers have unique responsibilities for both domestic and international privacy matters.
3. Copies of the Treaty text will be tabled in parliament. The Department of Home Affairs will prepare a National Interest Analysis.
4. Any agreement will be referred to the Joint Standing Committee on Treaties (JSCOT) for consideration. Stakeholders and members of the public will be able to make submissions to JSCOT indicating any privacy concerns that JSCOT will take into account before providing its recommendations.
5. Before Australia can ratify an Agreement, Regulations will be made under the TIA Act to declare the agreement as a 'designated international agreement'. Such Regulations will be subject to the normal disallowance periods in parliament, and to oversight by parliamentary committees such as the Parliamentary Joint Committee on Human Rights.

Accordingly, there will be considerable opportunities for the Australian Parliament and the Australian community to scrutinise proposed agreements that go to facilitating efficient and effective access to electronic data to combat serious crime.

A thorough assessment will be conducted of applicable domestic laws and policies of the foreign government before entering into any agreement. This will be supported by a range of safeguards and restrictions to reflect in those agreements Australian values such as rule of law, privacy considerations and that electronic surveillance powers be exercised under a purported agreement where it is necessary, proportionate and reasonable.

1.132 The committee requests the minister's more detailed advice regarding why it is considered necessary and appropriate to allow information held in Australia to be accessed by foreign governments in circumstances where existing legislative protections for the accessing of

information have been removed and no safeguards are provided on the face of the bill to ensure a designated international agreement contains sufficient safeguards regarding the circumstances in which information can be accessed.

Our collective safety and security depends on the ability of Australian agencies to maintain lawful and efficient access to electronic evidence. The Bill creates a framework for ensuring that Australia can enter into international cross-border access to data agreements with trusted foreign countries while respecting privacy interests and foreign sovereignty. However, the benefits of allowing Australian law enforcement agencies and ASIO to be able to directly issue orders on foreign providers, cross-border arrangements and agreements would need to be reciprocal.

For example, in order for Australia to be a qualifying foreign government that is able to enter into an agreement under the United States Clarifying Lawful Overseas Use of Data (CLOUD) Act, it must ensure the removal of blocking statutes. Blocking statutes are laws that would prevent the United States Government from issuing legal process directly on Australian providers to access electronic information held in Australia. Accordingly, it was necessary that amendments be made to the *Telecommunications Act 1997* to clarify that disclosures would be authorised by law for the purposes of the *Privacy Act 1988* so as to ensure that Australian providers were legally able to comply with such legal process.

The Bill sets the outer framework for these agreements, whilst the treaty negotiation process and the agreements themselves will provide flexibility for Australia to ensure that individual agreements reflect appropriate safeguards and restrictions, and the changing technological environment. Agreements negotiated will have a range of safeguards and restrictions to ensure respect for privacy and civil liberties, rule of law, requirements for appropriate thresholds, and independent authorisation processes, to ensure orders are reasonable, necessary and proportionate. These necessary safeguards set an important foundation for future negotiations of cross-border access to data agreements with like-minded foreign governments.

1.133 The committee also requests the minister's advice as to whether the bill can be amended to:

- **set out minimum protections and safeguards related to privacy that must be included in designated international agreements;**
- **specify that designated international agreements must be tabled in the Parliament; and**
- **provide that any regulation that specifies the name of a designated international agreement does not commence until after the Parliament has had the opportunity to scrutinise the designated international agreement.**

The Government considers that the current framing of the Bill permits sufficiently strong protections and safeguards to be agreed on between governments when negotiating cross-border access to data agreements. Australia's treaty-making process requires that all treaties be subject to Parliamentary scrutiny, including tabling in Parliament. Ordinarily, the treaty text is tabled before the Parliament to ensure transparency and allow for Parliamentary scrutiny processes to occur.

Please refer to the response under 1.131 detailing the available opportunities that the Australian Parliament would have to scrutinise any cross-border access to data agreements that the Government pursues.

Annexure A –Comparison table: Authorising authorities under the international production order framework and the domestic TIA Act framework

International production order authorising authorities			
	Law enforcement orders	**National Security orders**	**Control Order international production orders**
Interception international production order	Under clause 30, may be issued by eligible judges (clause 14) and nominated AAT members (clause 15)	Under clause 89, nominated AAT Security Division member (clause 17) (ASIO must first seek consent of the Commonwealth Attorney-General to make the application)	Under clause 60, may be issued by eligible judges (clause 14) and nominated AAT members (clause 15)
Access to stored communications international production order	Under clause 39, may be issued by issuing authorities (clause 16) (this includes magistrates, judges and certain AAT members)	Under clause 98,nominated AAT Security Division member (clause 17) (ASIO must first seek consent of the Commonwealth Attorney-General to make the application)	Under clause 69, may be issued by issuing authorities (clause 16) (this includes magistrates, judges and certain AAT members)
Access to telecommunications data international production order	Under clause 48, may be issued by issuing authorities (clause 16)	Under clause 107, nominated AAT Security Division member (clause 17)	Under clause 78, may be issued by issuing authorities (clause 16)

Current TIA Act authorising authorities			
	Law enforcement warrants	**National Security warrants**	**Control order warrants**
Interception warrants	Eligible Judges (section 6D) and nominated AAT members (section 6DA)	The Commonwealth Attorney-General (section 9)	Eligible Judges (section 6D) and nominated AAT members (section 6DA)
Access to stored communications warrant	Issuing authorities (section 6DB) (this includes magistrates, judges and certain AAT members)	N/A – access to stored communications currently granted under an interception warrant under section 9	Issuing authorities (section 6DB) (this includes magistrates, judges and certain AAT members)
Access to telecommunications data authorisation	Authorised officers of enforcement agencies (section 5AB) (this includes management offices or management positions of an enforcement agency or authorised senior executive member of the AFP, as authorised by the head of an enforcement agency or AFP Commissioner)	Eligible person (sections 175 and 176) (this includes the Director-General of Security, the Deputy Director-General of Security and ASIO employees or ASIO affiliates who covered by a relevant approval from the Director-General)	No specific data authorisation for control orders