



## **Australian Government**

Australian Government response to the Parliamentary Joint  
Committee on Intelligence and Security:

Advisory Report on the *Surveillance Legislation Amendment (Identify  
and Disrupt) Bill 2020*

NOVEMBER 2025

**Recommendations made in the Advisory Report on the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020***

**Committee Recommendations**

**Recommendation 1:**

The Committee recommends that, in line with the proposed expansion of the *Inspector-General of Intelligence and Security's* oversight role, the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*, the *Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020* and, to the extent necessary, other legislation be amended to expand the oversight remit of the Parliamentary Joint Committee on Intelligence and Security to cover the intelligence functions of the ACIC (including, but not limited to, the use of network activity warrants by the ACIC).

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

**Recommendation 2:**

The Committee recommends that the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*, the *Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020* and, to the extent necessary, other legislation be amended to expand the oversight remit of the Parliamentary Joint Committee on Intelligence and Security to cover the intelligence functions of the AFP (including, but not limited to, the use of network activity warrants by the AFP).

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 3:**

The Committee recommends that the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*, the *Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020*) and, to the extent necessary, other legislation be amended to extend the oversight remit of the *Inspector-General of Intelligence and Security's* oversight to include all intelligence functions of the AFP (including, but not limited to, not the use of just network activity warrants).

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 4:**

The Committee recommends the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* and, to the extent necessary, other legislation be amended to expand the inspection mandate and functions of the Commonwealth Ombudsman to cover – in explicit terms – the propriety of the AFP and ACIC's actions, practices, policies and activities under these new powers.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 5:**

The Committee recommends that, where a Bill proposes to give operational or intelligence agencies specific new or expanded powers, those agencies should, in addition to providing input to any departmental submission, provide a separate unclassified submission to the Committee which should, at least, outline the necessity and proportionality of the proposed new or expanded powers. Such a submission should include, where appropriate, case studies on the current environment and how the use of any proposed new or expanded powers will assist the agency in the carrying out of its functions. The Committee also recommends that the Department of Home Affairs not make any further submission to the Committee that purports to be authored by, or submitted on behalf of, the "Home Affairs Portfolio." For the avoidance of doubt this recommendation should not preclude an agency providing a classified submission in addition to any unclassified submission.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 6:**

The Committee recommends that, in support the proposed expansion of the Parliamentary Joint Committee on Intelligence and Security's oversight remit (see Recommendations 1 and 2), the AFP and the ACIC provide an unclassified annual report to the Committee which sets out:

- to the extent it is possible to do so in an unclassified report, similar information to what is required to be provided under section 3ZZVL of Schedule 3 of the *Surveillance Legislation Amendment (Identify and xvii Disrupt) Bill 2020* (except that information should be provided in respect of all three of the new powers rather than just the account takeover warrants); and
- the offences in respect of which the warrants were sought or obtained.

This new reporting requirement should be supplemented by classified briefings to the Committee outlining the use of the new powers and their relationship both to each other and other existing powers provided to the AFP and ACIC.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 7:**

The Committee recommends the *INSLM Act* be amended to provide for INSLM review of the data disruption, network activity and account takeover warrants introduced by the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* within three years of the Bill receiving Royal Assent. The Committee further recommends that the *INSLM Act* be amended to require the INSLM to provide a copy of his or her report to the Committee at the same time the report is provided to the Minister.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 8:**

The Committee recommends the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be amended so that the Parliamentary Joint Committee on Intelligence and Security may conduct a review of the data disruption, network activity and account takeover warrants not less than four years from when the Bill receives Royal Assent to allow the Committee to take into account any report by the INSLM. In addition the Committee recommends that the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be amended so that each of the new powers sunset five years from the date on which the Bill receives Royal Assent.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 9:**

The Committee recommends the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be amended so that the issuing authority for all of the new powers introduced by the Bill, including emergency authorisations, must be a superior court judge (either of the Federal Court or a State or Territory Supreme Court), except for Account Takeover Warrants which may be granted by an Eligible Judge per Section 12 of the Surveillance Devices Act 2004 (Cth).

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 10:**

The Committee recommends the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be amended to provide additional requirements on the considerations of the issuing authority to ensure the offences are reasonably serious and proportionality is maintained. The effect of any changes should be to strengthen the issuing criteria and ensure the powers are being used for the most serious of offending.

- This should include specific consideration as to whether the offending relates substantially to: offences against the security of the Commonwealth per Chapter 5 of the Criminal Code; offences against humanity including child exploitation and human trafficking per Chapter 8 of the Criminal Code; serious drug, weapons and criminal association offences per Chapter 9 of the Criminal Code; and money laundering and cybercrime offences per Chapter 10 of the Criminal Code. These examples are not exhaustive, but designed to reflect the intention of the Bill as seen through the Explanatory Memorandum and evidence to this Committee.
- This should include the nature of the offending and its relationship to other serious offences.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 11:**

The Committee recommends the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be amended so that the issuing authority, to the extent known, must consider the following:

- consideration to third parties specifically, including their privacy;
- specific consideration of privileged and journalistic information; and,
- specific consideration of privacy impacts, financial impacts, and the ability of individuals to provide or receive care.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

## Recommendation 12:

The Committee recommends the Government commission a review of Commonwealth legislation to determine whether the concepts of “serious offence,” “relevant offence” and other similar concepts:

- should be made consistent across different *Acts of Parliament* (noting that, for example, the definition of “serious offence” in the *Telecommunications (Interception and Access) Act 1979* is different to the definition of “relevant offence” in the *Surveillance Devices Act 2004*; and
- whether the threshold for the concept of “serious offence” in all Commonwealth legislation should be – at a minimum – an indictable offence punishable by a maximum penalty of seven years’ imprisonment or more, with a limited number of exceptions.

This body of work should inform the eventual electronic surveillance bill being considered by the Department of Home Affairs and other departments.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

## Recommendation 13:

The Committee recommends the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be amended so that, in order to provide an emergency authorisation for disruption of data held in a computer:

- in addition to the matters set out in proposed section 28(1C) of the *Surveillance Devices Act 2004*, an authorising officer must be satisfied that there are no alternative means available to prevent or minimise the imminent risk of serious violence to a person or substantial damage to property that are likely to be as effective as data disruption; and
- the authorising officer must consider the likely impacts of the proposed data disruption activity on third parties who are using, or are reliant on, the target computer and be satisfied that the likely impacts on third parties are proportionate to the objective of the emergency authorisation.

In addition, the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* should be amended so that, where an issuing authority declines to retrospectively approve an emergency data disruption authorisation, the issuing authority may require the AFP or ACIC to take such remedial action as considered appropriate in the circumstances, including financial compensation.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

#### **Recommendation 14:**

The Committee recommends that the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be amended so that any post-warrant concealment powers must be exercised within 28 days after the relevant warrant has expired unless the AFP or the ACIC (as applicable) has obtained the approval of a superior court judge to undertake post-concealment activities at a later date. Consistent with the recommendation made by the INSLM, the superior court judge should be required to consider:

- how the AFP or the ACIC (as applicable) is proposing to conceal access;
- the likely privacy implications at the time and in the place where the concealment activity is proposed to occur; and
- whether, in all the circumstances, the concealment activity is appropriate.

In addition, and noting that the Committee did not receive evidence on concealment in relation to computer warrants, the Committee recommends that the Government consider whether the same amendment should be made in respect of computer access warrants in the *Surveillance Devices Act 2004* consistent with the recommendation made by the INSLM.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

#### **Recommendation 15:**

The Committee recommends the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be amended so that:

- for the purposes of proposed paragraphs 27KE(7)(b) and 27KE(12) (and any other relevant provision), a data disruption warrant may only authorise the AFP or ACIC to cause material loss or damage to other persons lawfully using a computer if the loss or damage is necessary to do one of the things specified in the warrant (i.e. it is not enough that the loss or damage is “justified and proportionate”); and
- the AFP and ACIC must notify the Commonwealth Ombudsman or IGIS (as appropriate) as soon as reasonably practicable if they cause any loss or damage to other persons lawfully using a computer.

The notification to the Commonwealth Ombudsman or IGIS (as applicable) must include, among other things, details of the loss or damage caused by the disruption activity and an explanation of why the loss or damage was necessary to do one of the things specified in the warrant.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 16:**

The Committee recommends that the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be amended so that the power to temporarily remove computers and other things from premises under a data disruption warrant or a network activity warrant must be returned to the warrant premises as soon as it is reasonably practicable to do so.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 17:**

The Committee recommends the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* should be amended to change the reporting requirements from the agencies to the Commonwealth Ombudsman from six-monthly to annually.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 18:**

The Committee recommends that the Government introduce legislation to implement the Committee's recommendations in its report on press freedom as soon as possible. In the meantime, the Committee recommends that the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be amended so that the issuing criteria for each of the proposed new powers requires the applicant, and the issuing authority, to consider the following matters in respect of any warrant that relates to – or may affect – a person working in a professional capacity as a journalist or a media organisation:

- the public interest in preserving the confidentiality of journalist sources; and
- the public interest in facilitating the exchange of information between journalists and members of the public to facilitate reporting of matters in the public interest.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 19:**

Consistent with Recommendation 2 of the Committee's report on press freedom, the Committee recommends that the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be amended to require that – with respect to an application for a data disruption warrant, a network activity warrant or an account takeover warrant that is being sought in relation to a journalist or media organisation – a “public interest advocate” be appointed.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 20:**

The Committee recommends that the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be amended to make clear the issuing criteria for an assistance orders also requires the issuing authority to be satisfied that:

- the order for assistance – and not just the disruption of data – is:
  - reasonably necessary to frustrate the commission of the offences that are covered by the disruption warrant; and
  - justifiable and proportionate, having regard to (i) the seriousness of the offences that are covered by the disruption warrant and (ii) the likely impacts of the data disruption activity on the person who is subject to the assistance order and any related parties (including, if relevant, the person's employer) and (iii) the likely impacts of the data disruption activity on other persons, including lawful computer users or clients of the person subject to the order; and
- compliance with the request is practicable and technically feasible (noting that these criteria are to be found in the industry assistance measures introduced by the *Assistance and Access Act 2018*).

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 21:**

The Committee recommends the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be amended to require consideration by the issuing authority, to the extent that is possible, of whether a person is, or has been, subject to other mandatory assistance orders (including mandatory assistance orders made under other Commonwealth legislation). Having regard to the covert nature of mandatory assistance orders, and the fact that it may not be possible for the issuing authority or applicant to have knowledge of previous (or even concurrent) orders, the Committee further recommends that the Government develop a mechanism to ensure that individuals and companies are not subject to multiple mandatory assistance orders unless specific consideration is given to whether, in all of the circumstances, it is reasonably necessary and proportionate.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 22:**

The Committee recommends the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be amended to:

- impose a maximum period during which a non-emergency mandatory assistance order may be served and executed (and if the order is not served and executed within that period, the order will lapse and a new order must be sought);
- require all applications for a non-emergency mandatory assistance order to be made in writing;
- require all applications for a non-emergency mandatory assistance order to include, to the extent known key particulars, including the nature of the mandated assistance;
- prohibit the AFP and the ACIC, unless absolutely necessary, from seeking a non-emergency mandatory assistance order in respect of an individual employee of a company (i.e. assistance should only ever be sought from the company or business);
- set out the process that must be followed in respect of the service of a non-emergency mandatory assistance order on the specified persons, and link the commencement of an order to the date and time of service; and
- require that an issuing authority consider whether a person is, or has been subject, to a non-emergency mandatory assistance orders (including mandatory assistance orders made under other Commonwealth legislation).

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 23:**

The Committee recommends that the Government make clear that no mandatory assistance order, including those defined in the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*, can ever be executed in a manner that amounts to the detention of a person.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 24:**

The Committee recommends the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be amended to introduce good faith immunity provisions for both assisting entities and those employees or officers of assisting entities who are acting in good faith with an assistance order.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 25:**

The Committee recommends the Explanatory Memorandum to the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be amended to make it clear that decisions under the proposed new powers are not excluded from judicial review under the *Administrative Decisions (Judicial Review) Act 1977 (ADJR Act)*.

For the avoidance of doubt, the Committee believes that no decision made in relation to data disruption warrants, network activity warrants and account takeover warrants should be exempt from judicial review under the *ADJR Act*.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 26:**

The Committee recommends proposed paragraph 27KA(3)(b) of the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be amended to provide that the statement of facts and grounds accompanying all applications for data disruption warrants must specify the following matters to the extent that is possible:

- the acts or types of acts of data disruption that are proposed to be carried out under the warrant;
- the anticipated impacts of those specific acts or types of acts of disruption on the commission of the relevant offence (that is, how they are intended to frustrate that offence); and
- the likelihood that the relevant acts or types of acts of disruption will achieve that objective.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 27:**

The Committee recommends the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be amended so that only individuals who satisfy the following requirements may apply for a data disruption warrant or an account takeover warrant:

- the person is a law enforcement officer in relation to the AFP or ACIC (as applicable) within the meaning of section 6A of the *Surveillance Devices Act 2004*;
- the person has been individually approved, by written instrument made by the AFP Commissioner or ACIC CEO (as applicable) to apply for data disruption warrants; and
- the relevant agency head is satisfied that the person possesses the requisite skills, knowledge and experience to make warrant applications, and the person has completed all current internal training requirements for making such applications.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 28:**

The Committee recommends that paragraph 27KC of the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be amended so that, rather than a judge having to be satisfied, that a data disruption warrant would be “justifiable and proportionate”, the judge must be satisfied, to the extent possible at the time an application is made, that a data disruption warrant is:

- reasonably necessary to frustrate the commission of the offences referred to in the warrant application; and
- proportionate, having regard to:
  - the specific nature of the proposed disruption activities;
  - the proportionality of those activities to the suspected offending;
  - the potential adverse impacts of the disruption activities on non-suspects; and
  - the steps that are proposed to be taken to avoid or minimize those adverse impacts, and the prospects of those mitigating steps being successful.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 29:**

The Committee recommends the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* and the *IGIS Act* be amended to make it clear that staff members of the *Australian Signals Directorate* are subject to IGIS oversight if they are seconded to the AFP or ACIC to execute a data disruption warrant for and on behalf of the AFP or ACIC.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 30:**

The Committee recommends the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be amended to strengthen the issuing authority considerations for network activity warrants, including by amending the definition of a “criminal network of individuals” to require there to be a reasonable suspicion of a connection between:

- the suspected conduct of the individual group member in committing an offence or facilitating the commission of an offence; and
- the actions or intentions of the group as a whole.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 31:**

The Committee recommends the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be amended to clarify that a decision-maker, and the issuing authority, must consider the privacy implications to the extent they are known, of a proposed network activity warrant.

To be clear, the committee does not believe that privacy considerations should be determinative in their own right, just that they should be considered.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 32:**

The Committee recommends the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be amended to require a sworn affidavit setting out the grounds of an application for an account takeover warrant (consistent with the delayed notification search warrants in the *Crimes Act*).

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

### **Recommendation 33:**

The Committee recommends that the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be amended to require an issuing authority to consider, to the extent that is possible at the time the application is made, whether a proposed account takeover warrant is likely to have an adverse impact on third parties, including a specific requirement to assess the likely:

- impacts on personal privacy;
- financial impacts on individuals and businesses;
- impacts on a person's ability to conduct their business or personal affairs; and
- impacts on a person's ability to have contact with family members or provide or receive care.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

**Recommendation 34:**

The Committee recommends the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be passed, subject to the amendments outlined above.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.