Australian Government

Australian Government response to the Independent National Security Legislation Monitor:

Review of the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*

NOVEMBER 2025

Australian Government response to the Independent National Security Legislation Monitor review

Introduction

The Australian Government thanks the Independent National Security Legislation Monitor (the Monitor) for his report, *Data Disruption, Network Activity and Account Takeover Powers: Review of Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*. The Government would like to acknowledge the contributions that organisations made both in attending hearings and preparing written submissions to the Monitor's inquiry.

In his review the Monitor found that the powers introduced by the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (SLAID Act) have been effective in helping to identify and disrupt serious crime and that there is a strong case for maintaining them. The Monitor also made a number of recommendations relating to enhancing the system for issuing warrants and improving the safeguards that apply to SLAID Act powers, but are also common to all electronic surveillance warrants.

In response to the Monitor's 21 recommendations, the Government has agreed to 4 of those recommendations, agreed 2 recommendations in part, and noted the remaining 15. The Government will further consider the recommendations that have been agreed in part or noted, as part of electronic surveillance reform, as these recommendations are applicable to the electronic surveillance framework as a whole. The four recommendations accepted by the Government included contingent recommendations from the INSLM—they contemplate other recommendations (namely recommendations 6-8) also being implemented. Those other recommendations have been noted and will be considered during electronic surveillance reform, given their potential applicability to a wide range of electronic surveillance powers.

Many of the Monitor's recommendations intersect with policy and legislative matters already under consideration as part of broader reform, in particular, the implementation of the 2019 *Comprehensive Review of the Legal Framework of the National Intelligence Community*, conducted by Mr Dennis Richardson AC (the Comprehensive Review) and the 2024 *Independent Review of the Australian Criminal Intelligence Commission and associated Commonwealth law enforcement arrangements* (the ACIC Review). The SLAID Act powers are often used in conjunction with other electronic surveillance powers, and it is therefore important to ensure that the framework governing their use is consistent with these broader reforms.

The Government is pleased to provide the following response to the Monitor's recommendations.

Recommendations

Recommendation One

The Monitor recommends that the AFP should retain DDWs, subject to recommendations 6–8 being implemented. ACIC should not retain the ability to use DDWs.

The Government **agrees** to this recommendation.

The Government agrees that the Australian Federal Police (AFP) should retain the power to obtain and use Data Disruption Warrants (DDWs) as they are a critical tool that enables the AFP to prevent serious technology enabled criminal activity and minimise harm to victims.

The Government will extend the sunsetting date, which is currently 4 September 2026, in the first instance, to allow recommendations 6–8 to be further considered as part of comprehensive reforms to the electronic surveillance framework recommended by the Comprehensive Review (electronic surveillance reforms). This will ensure that the recommendations relating to how warrants are issued can be considered in the context of the framework as a whole, before any decision is made on making the powers a permanent part of the statutory framework.

On 14 November 2024 the Government published its response to the *Independent Review of the Australian Criminal Intelligence Commission and associated Commonwealth law enforcement arrangements* (the ACIC Review). In response to the ACIC Review, the Government agreed that disruption operations should remain the responsibility of law enforcement agencies. Consistent with that position and the Australian Criminal Intelligence Commission (ACIC)'s transition from a law enforcement agency to a criminal intelligence agency with powers that support it to effectively fulfil this remit, the Government agrees that the ACIC no longer requires the ability to use DDWs. The Government intends to discontinue ACIC's access to DDWs in advance of the finalisation of other reform projects, noting work is underway to develop new governing legislation for the ACIC to ensure it has access to powers with appropriate thresholds for its intelligence focus.

Recommendation Two

The Monitor recommends that the ACIC and AFP should retain NAWs, subject to recommendations 6–8 being implemented.

The Government **agrees** to this recommendation.

The Government agrees that both the AFP and the ACIC should retain access to Network Activity Warrants (NAWs). NAWs have proven to be an effective, necessary and proportionate capability to collect intelligence on serious cyber-enabled and cyber-dependent criminal activity that could not have been gathered using traditional surveillance warrants. NAWs enable agencies to identify and understand criminal networks in an online environment where the use of anonymising technologies continues to grow.

As previously stated, the Government will extend the sunsetting date, to allow further work to consider recommendations 6–8 to be undertaken as part of electronic surveillance reform.

Recommendation Three

The Monitor recommends that both ACIC and AFP should retain ATWs, subject to recommendations 6–8 being implemented. In the case of ACIC, ATWs should be for intelligence rather than evidence collection purposes.

The Government **agrees** to this recommendation.

The Government agrees that access to Account Takeover Warrants (ATWs) should be retained by both the AFP and the ACIC.

ATWs have proven to be an effective capability enabling the AFP to collect evidence about a person's online criminal activity and identify potential victims. The ACIC has demonstrated the continued utility of ATWs for intelligence purposes, particularly in light of the continued growth in cyber-enabled and cyber-dependent crime.

As previously stated, the Government will extend the sunsetting date, to allow further work to consider recommendations 6–8 to be undertaken as part of electronic surveillance reform.

Recommendation Four

The Monitor recommends that the named person ATWs should be introduced for AFP and ACIC, subject to recommendations 6–8 and the following additional safeguards:

a) Available only where the use of an account-based ATW would be ineffective.

b) A certification process for adding accounts based on the same criteria used to issue ATWs.

c) Additional record keeping and reporting requirements.

The Government **notes** this recommendation.

The Government will undertake further work to consider this recommendation, along with recommendations 6–8, as part of electronic surveillance reform to ensure consistency across the entire electronic surveillance framework.

Recommendation Five

The Monitor recommends that the maximum duration of NAWs should be extended to 6 months, subject to recommendations 6–8 and a mechanism to ensure 6 monthly reporting.

The Government **agrees** to this recommendation.

The Government agrees to extend the duration of NAWs to better reflect their purpose as an intelligence warrant and to enhance operational planning and effectiveness of the NAW as an intelligence collection authority.

The Government will undertake further work on this recommendation, as part of electronic surveillance reform and the implementation of the Government response to the ACIC Review.

Recommendation Six

The Monitor recommends that the issuing authorities should be retired judges. If this is not accepted, then it should be current judges for all SLAID Act warrants. In either case they must be supported by PIMs and technical advisors.

The Government **notes** this recommendation.

The Government acknowledges that the system for issuing warrants should ensure that issuing authorities have complete and accurate information, and the requisite independence and skills to make fair decisions in a timely manner. These mechanisms are important to ensure that the use of the covert and intrusive powers is proportionate and promote public confidence. The current issuing arrangements, which involve federal judges acting *persona designata* and nominated, legally-qualified members of the Administrative Review Tribunal issuing SLAID Act warrants, are consistent with those for warrants across the electronic surveillance framework.

This recommendation will be considered as part of the broader electronic surveillance reform to ensure that the issuing arrangements and safeguards for SLAID Act warrants align with the arrangements for other electronic surveillance warrants. As the Monitor notes, there would be significant practical challenges in maintaining an independent body that considers only the small number of SLAID Act warrants issued annually.

Recommendation Seven

The Monitor recommends that there should be Public Interest Monitors whose role includes providing submissions on matters of public interest and feedback from oversight processes, identifying matters where independent technical advice may be required and providing comments on draft warrant applications and templates.

The Government **notes** this recommendation.

Electronic surveillance reform will holistically consider safeguards to ensure alignment for all electronic surveillance warrants and this may include considerations as to the establishment of a Commonwealth PIM. It would be critical to ensure that any Commonwealth PIM does not detract from operational efficiency, or the timely issue of warrants in time-critical operations.

This consideration will include consultation with states and territories as to how a Commonwealth PIM may interact with state PIMs. Close consultation with issuing authorities, the Ombudsman, and the Inspector-General of Intelligence and Security would also be needed to ensure that, should a PIM model be established, there is no overlap or duplication of responsibilities.

Recommendation Eight

The warrant issuing system also requires:

a) A mechanism for access to independent technical advice.

b) A statutory duty of candour requiring disclosure of all matters of which the applicant is aware, both favourable and adverse.

c) That warrant applications are independently allocated to issuing authorities.

d) An effective secretariat should be established with functions that include the allocation of warrants, case management and data collection.

The Government **notes** this recommendation.

As discussed in response to recommendation 6, the Government recognises the importance of a robust system for the independent authorisation of electronic surveillance and disruption powers. The Government notes that the AFP and ACIC have a longstanding practice of operating in a manner that is consistent with them owing a duty of candour and that, in making his recommendation, the Monitor has not identified any evidence to suggest that the AFP or ACIC have failed to display candour in their applications.

The system for issuing warrants, including the information that must be supplied to issuing authorities as part of an application, will be considered through electronic surveillance reform to ensure consistency across the framework.

Recommendation Nine

The Monitor recommends that warrants should only be available for offences punishable by 5 or more years imprisonment.

The Government **notes** this recommendation.

The Comprehensive Review recommended that electronic surveillance powers should only be available for offences punishable by 5 or more years of imprisonment, with limited exceptions for specified offences for which the use of such powers is typically necessary. Recommendation 9 will be considered as part of broader electronic surveillance reform alongside the Comprehensive Review recommendation.

The Government notes that the ACIC – as a criminal intelligence agency – will require a separate threshold aligned with its functions, rather than a threshold oriented at the

investigation of offences. This threshold will be considered through the Government response to the ACIC Review.

Recommendation Ten

The Monitor recommends that the expression 'criminal network of individuals' should be renamed 'targeted network' or something similar that does not misleadingly imply that all persons using the same electronic service is suspected of being engaged in criminal activity.

The Government **notes** this recommendation.

The Government acknowledges that clarity in the law is important, to support public understanding—in particular in relation to covert and intrusive powers, such as NAWs. Definitions will be considered through electronic surveillance reform.

Recommendation Eleven

The Monitor recommends that for urgent applications the issuing authority should be satisfied that there is a reasonable basis for both the 'impracticality' and the 'urgency' criteria.

The Government **notes** this recommendation.

The Government acknowledges that the criteria for urgent applications should be consistent between ATWs (which do not expressly require the issuing authority to be satisfied of the 'impracticality' criteria) and NAWs and DDWs (where 'impracticality' is required).

The Government notes that the Comprehensive Review made detailed recommendations about the design of approval processes for warranted powers in time-sensitive cases and emergencies.

The Government notes that the design of approval processes will be considered through electronic surveillance reform to ensure consistency across the framework.

Recommendation Twelve

Issuing criteria should require that the issuing authority is satisfied that the warrant is necessary and proportionate in all the circumstances. In assessing necessity and proportionality, the list of matters to be considered should include the: a) nature and gravity of the offences being investigated (or disrupted); b) likelihood that the proposed activity will succeed as well as the likely value of the resulting intelligence, evidence or disruption; c) extent to which the privacy of any person is likely to be interfered with; d) extent to which property rights are likely to be interfered with, including through introduction of vulnerabilities;

e) likelihood of special categories of information including information subject to LPP and information about journalists' sources being collected and, if it is, how the information will be protected; and

f) existence of any alternative, less intrusive means of obtaining the information.

The Government **notes** this recommendation.

The Government recognises that clear and simple issuing criteria may enhance legal certainty.

The Government notes that policy intent for the issuing authority to consider the privacy implications 'to the extent known' was not intended to reverse the onus of proof for NAWs. The nature of NAWs means that the full privacy implications are not always known, meaning the legislation must be framed to ensure that the decision maker is not obliged to make a decision based on unknown events.

The Comprehensive Review made detailed recommendations about the design of warrant tests, including the introduction of a statutory necessity and proportionality test supported by matters that issuing authorities must take into account in particular cases. As such, the detailed design of warrant tests will be considered through electronic surveillance reform.

Recommendation Thirteen

The Monitor recommends that DDWs should only be available when other measures would not be effective.

The Government **notes** this recommendation.

The Government notes that it is the practice of the AFP to only seek a DDW in situations where other mechanisms are not likely to be effective.

Consideration of the detailed design of warrant tests will be undertaken through electronic surveillance reform. Any additional issuing criteria should not require AFP to exhaust all other options in order to access DDWs.

Recommendation Fourteen

The Monitor recommends that the secrecy provisions should be reformed in accordance with the following principles:

a) Removal of unnecessary complexity and inconsistency.

b) Reliance on the general secrecy offences in the Criminal Code.

c) Retention of strict limits on the way officials can use information obtained under warrants, potentially through positively defining what use is permitted in the 'course of duties.'

d) There should be no barrier to a person seeking legal advice about an assistance order they may be required to comply with.

e) Potentially exculpatory material obtained under a NAW should be able to be disclosed in accordance with the usual prosecutorial duty of disclosure.

f) The law should be clarified to put beyond doubt that NAW information cannot be admitted in evidence in proceedings under the *Proceeds of Crime Act 2002* (Cth).

The Government **agrees** to recommendations (d) and (e), and **notes** recommendations (a), (b) (c) and (f).

In relation to recommendations (a) to (c), strict limits on the way officials can use information obtained under SLAID Act warrants are necessary to safeguard people's right to privacy and ensure that the exercise of SLAID Act powers is necessary and proportionate. Further, clear and coherent secrecy offences, and use and disclosure provisions are important to promote legal certainty.

The simplification of secrecy, use and disclosure provisions across the electronic surveillance framework was also a central recommendation of the Comprehensive Review. A detailed design and update of the use and disclosure framework will be considered as part of electronic surveillance reform. Any amendments to secrecy offences will also need to be consistent with the principles in the Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers.

In relation to recommendation (d), the Government agrees that a person who is served with an assistance order should be able to seek legal advice in relation to the order. Paragraphs 45B(4)(aa) and 45B(4)(a) of the *Surveillance Devices Act 2004* (SD Act) currently permit the use and disclosure of information in connection with the administration or execution of the Act and this was intended to include seeking legal advice. The Government will consider whether amendments to clarify this position are desirable, as part of electronic surveillance reform.

Urgent amendments were progressed to implement recommendation (e) in Schedule 1 to the *Telecommunications and Other Legislation Amendment Act 2025* which commenced on 5 November 2025. These amendments ensure that exculpatory material obtained under a NAW may be disclosed as part of the duty of disclosure and that such evidence is admissible into evidence where necessary to protect the defendant's right to a fair trial and the interests of justice.

The Government will consider recommendation (f) through electronic surveillance reform. As noted in the Monitor's report, the SLAID Act was not intended to allow NAW information to be used in proceedings under the *Proceeds of Crime Act 2002* (POCA), and the AFP has not used NAW information in such proceedings. In considering this recommendation, it would be necessary to ensure that legislative amendments do not inadvertently unduly limit the legitimate use of such information. For example, subsection 45B(10) of the SD Act is intended to allow NAW information to be admitted into evidence in

a proceeding that is not a criminal proceeding in order to allow for protected network activity warrant information to be admitted into other hearings, such as those that question the validity of the warrant. Any prohibition against NAW information being admitted in evidence in proceedings under the *Proceeds of Crime Act 2002* (POCA) would need to ensure that NAW information can be used in POCA proceedings, should there be a challenge to the validity of a warrant in such proceedings.

Recommendation Fifteen

The Monitor recommends that the information accessed under a SLAID Act power should be reviewed at least every 5 years and destroyed if no longer required for identified purposes. Internal agency policies and/or binding administrative guidance should make provision for earlier reviews of particularly sensitive categories of information.

The Government **notes** this recommendation.

The Government acknowledges the need for safeguards to ensure any limitations imposed on the right to privacy by SLAID Act warrants are proportionate and appropriate and adapted to achieving a legitimate objective. The SLAID Act already requires agencies to cause the destruction of records or reports as soon as practicable and within five years unless the chief officer of the agency certifies that the record or report is still required for an authorised purpose.

The redesign of the destruction requirements will be progressed through electronic surveillance reforms to ensure a holistic approach.

Recommendation Sixteen

The Monitor recommends that further consideration should be given to issuing binding administrative guidance to provide additional protections for the collection, use, retention and disclosure of information, particularly personal and sensitive information.

The Government **notes** this recommendation.

Detailed rules regarding the collection, use, disclosure, retention and destruction of information obtained through these warrants is already embedded in the legislative frameworks for the use of these powers. The Government is considering the role of guidance relating to the ACIC's intelligence collection activities and its treatment and handling of information obtained – including material obtained under SLAID Act powers – via implementation of ACIC Review recommendations. Consideration of these issues with respect to the AFP will be progressed as part of electronic surveillance reform.

Recommendation Seventeen

The scheme for emergency authorisations should be amended so that:

a) Emergency authorisations are not available to ACIC.

b) The limitation preventing an issuing authority from ever requiring the destruction of information should be removed.

The Government **notes** this recommendation.

It is important to distinguish between emergency authorisations and time-sensitive authorisations. *Emergency authorisations* allow for internal authorisation to prevent or lessen harm in situations of genuine emergency, while *time-sensitive authorisations* provide a streamlined process to seek independent authorisation in cases where delay would adversely affect operational outcomes.

The Comprehensive Review recommended that a tiered authorisation framework for time-sensitive situations whereby:

- for law enforcement agencies, the issuing authority may issue the warrant based on an oral application if it is not possible to do so in writing, and
- for intelligence agencies, the Director-General may authorise activities in limited circumstances when the sole issuing authority (the Attorney-General) is unavailable.

The Comprehensive Review also recommended that law enforcement agencies be permitted to internally authorise the use of electronic surveillance powers in threat to life and other emergency situations. The Review noted emergency authorisation powers should be limited to law enforcement agencies that are responsible for taking action to prevent or lessen harm, and not be available in respect of intelligence powers.

Additionally, the Comprehensive Review recommended that issuing authorities be able to invalidate internally authorised uses of powers in emergency and time-sensitive cases, and require the destruction of information obtained if the issuing authority considers that the authorisation ought never to have been granted.

The Government will address the design of emergency and time-sensitive authorisations through the ACIC reform and electronic surveillance reform processes.

Recommendation Eighteen

The Monitor recommends that the scheme for assistance orders should be modified so that:

a) Assistance orders are to be only able to be issued when it is proportionate to do so.

b) Issuing authorities have express authority to place limits or conditions on assistance orders.

The Government **notes** this recommendation.

Assistance orders provide a mechanism for the AFP and ACIC to secure cooperation from a person with relevant technical knowledge of a computer or system which is often necessary for the execution of a warrant. The person from whom assistance is sought may not always be a designated communication provider and for this reason, the industry assistance regime in Part 15 of the *Telecommunications Act 1997* may not be sufficient.

The ability for an issuing authority to impose conditions or restrictions on the exercise of powers is commonly found in warrant and other similar frameworks. The Comprehensive Review contains detailed recommendations relating to design of warrant tests, including the introduction of a statutory necessity and proportionality test supported by matters that issuing authorities must take into account. For this reason, this recommendation will be considered as part of electronic surveillance reform.

Recommendation Nineteen

The Monitor recommends that the Ministerial reporting requirements should be retained and amended so that:

a) There are consistent reporting requirements across the SLAID Act warrants.

b) Reporting on named person ATWs includes details of the accounts that were taken over under the warrant and the reasons it would not have been effective to take over those accounts under a specified account ATW.

c) There is no more than 6 months between the warrant being issued and the requirement to provide a report to the Minister being triggered.

d) Individual reports on ATWs are required.

The Government **notes** this recommendation.

Ministerial reporting requirements are an important mechanism to provide accountability to the Parliament and protect the public interest.

The Comprehensive Review considers the Ministerial reporting requirements, including whether they provided meaningful information that enhances Parliamentary and public accountability.

Reporting requirements will be considered comprehensively through the ACIC and electronic surveillance reforms.

Recommendation Twenty

The Monitor recommends that the Public annual reporting requirements should be amended to include:

a) The number of warrants where specified categories of sensitive information is sought or is likely to be obtained (including LPP and journalist source information).

b) The number of people, devices and accounts affected by each category of warrant (NAW, DDW and ATW).

c) Reason for refusal of an ATW (consistent the existing requirement for DDWs and NAWs).

d) The number of occasions on which issuing authorities have required agencies to provide further information in support of warrant applications; the number of warrants granted with conditions; input of Commonwealth PIMs in warrant issuing; and, the work of the technical advisors.

e) The number of assistance orders sought, granted and used each year.

f) An annual statement that describes, as far as possible, how the use of each type of warrant has enhanced the ability of each agency to investigate, disrupt and prosecute (as relevant) serious crime.

g) A framework for deferred reporting based on that in s 50A of the SD Act.

The Government **notes** this recommendation.

The Government notes that public reporting is a key mechanism for promoting transparency, accountability and public trust in the use of covert powers by law enforcement. Public reporting enhances the understanding of the need for these powers, the way in which the powers are used and any trends in use. This plays a critical role in building and sustaining confidence in the legislative and operational framework.

Public reporting obligations for the use of covert and intrusive powers including SLAID Act warrants will be considered in conjunction with electronic surveillance reform to ensure consistency across the framework.

Recommendation Twenty-one

The Monitor recommends that the oversight arrangements should be modified to reflect the following:

a) There should be no statutory barrier to IGIS, the Ombudsman, PIMs and the technical advisors sharing relevant information.

b) Oversight bodies and the INSLM should have access to the proposed technical advisors.

c) Existing prescriptive requirements for Ombudsman inspections should be repealed and replaced by the ability to conduct inspections to examine matters akin to those that the Ombudsman can currently consider in 'investigations'.

d) Prescriptive statutory record keeping and notification requirements should be replaced by a scheme that allows for binding administrative guidance to be given and updated as required.

e) IGIS and the Ombudsman should be able to brief parliamentary committees and IGIS should be able to publish unclassified inspections reports and inquiries at any time.

f) There should be consistent obligations on the Ombudsman to not include sensitive DDW or ATW information in public reports.

The Government **agrees** to recommendation (a), and **notes** the other parts of the recommendation.

The Government acknowledges the importance of equipping IGIS and the Ombudsman with the necessary powers and information to carry out their functions under the Act, including the power to share information on inter-related responsibilities to facilitate effective oversight.

With respect to the Monitor's recommendations in (a), the Strengthening Oversight of National Intelligence Community Bill 2025 (SONIC Bill) includes transitional provisions to facilitate information-sharing between the Ombudsman and the IGIS, noting the SONIC Bill would expand the jurisdiction of the IGIS to include, relevantly, the ACIC and the intelligence functions of the AFP. Beyond the conclusion of the transitional provisions, the Bill would permit the sharing of information concerning the ACIC and the AFP between the IGIS and the Ombudsman where it is relevant to their respective functions.

In relation to recommendation (b), this will be considered further by Government as part of its electronic surveillance reform, to ensure a consistent approach for oversight of electronic surveillance powers.

In relation to recommendation (c), the Comprehensive Review recommended that the Ombudsman's oversight powers be expanded, and that it be given the power to examine the legality of law enforcement agencies' use of electronic surveillance powers. The Government acknowledges that a closer alignment between the Ombudsman's inspection powers under the SD Act and its investigation powers under the *Ombudsman Act 1976* would be beneficial in ensuring the Ombudsman has flexibility in its oversight of the use of SLAID Act powers.

In relation to recommendation (d), the Comprehensive Review also considered that legislation and/or guidelines should be clear about record-keeping requirements, to support meaningful oversight.

In relation to recommendation (e), the SONIC Bill will amend the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act) to require the IGIS to brief the PJCIS at least once per year and the other aspects of this proposal will be considered as part of the electronic surveillance reform.

The oversight arrangements and reporting requirements for oversight bodies will be considered holistically and comprehensively through electronic surveillance reform.