

UNCLASSIFIED

Comprehensive Summary of AFP online 'Authorised Officer training' program and AFP Authorising Officers Telecommunications Interception Division Handbook (TID Handbook)

Overview of documents

The AFP training program is delivered online and provides the key points and considerations necessary to perform the duties of an Authorised Officer (AO) under relevant legislation. The online training program is mandatory, for all EL/SES sworn members and any sworn member acting in the capacity of an AO. This online training package must be re-validated every year.

In order to complete the training, AOs need to provide responses to questions based on the content.

The TID Handbook is a more detailed, 30 page guidance document available on the AFP intranet and is updated regularly. It is provided in support of the online training package.

Purpose of documents

The TID Handbook and training program provide support to AFP Authorised Officers (AO) with information and considerations necessary to perform the duties of an AO Officer under the *Crimes Act 1914*, the *Telecommunications (Interception and Access) Act 1979*, and the *Surveillance Devices Act 2004*, with **key learning objectives** for AOs being:

- Understand the relevant legislative powers , including obligations and threshold requirements;
- Understand the significant compliance requirements and potential adverse consequences of authorising a power incorrectly;
- Understand reporting requirements and oversight arrangements; and
- Know where to find assistance and resources to meet obligations.

Regimes Covered

The applicable legislative regimes provide powers to covertly capture evidence and information, ensuring justification, oversight and accountability to safeguard the privacy of the Australian community.

Under the *Crimes Act 1914*:

- Controlled Operation
- Major Controlled Operation
- Delayed Notification Search Warrants

Under the *Telecommunications (Interception and Access) Act 1979 (TIA Act)*:

- Telecommunications Interception Warrants
- Stored Communications Warrants
- Data Authorisations
- Journalist Information Warrants
- Control Order Interception Warrants

Under the *Surveillance Devices Act 2004 (SD Act)*:

- Surveillance Device Warrants
- Tracking Device Authorisations

UNCLASSIFIED

Topics covered

The topics covered in the TID Handbook and training program include detailed guidance for the Authorising Officer to consider in exercising powers. In relation to each regime, the material covered includes:

- Responsibilities of an Authorised Officer
- Reporting and Commonwealth Ombudsman Inspections
- Controlled Operations
 - *Controlled operation*
 - *Major controlled operation*
 - *Variation of authority by appropriate authorising officer*
 - *AFP variation of authority*
 - *Urgent controlled operations authorities and variations*
 - *Cancellations*
 - *Granting an authority*
 - *Granting an urgent authority*
- Telecommunications Interception Warrants
 - *Enabling and Disabling services and/or devices*
 - *Application for a warrant by telephone*
- Stored Communications and Preservation Notices
 - *How do Preservation Notices relate to Stored Communications Warrants?*
 - *Types of Domestic Preservation Notices*
 - *Foreign Preservation Notices and Stored Communications Warrants*
- Data Authorisations
 - *Data Retention*
 - *Who can authorise data authorisations*
 - *Issuing Data Authorisations – Domestic*
 - *Issuing Data Authorisations - Foreign*
 - *Restrictions*
 - *When is access to historic telecommunications data permitted?*
 - *Historic data requests relating to the enforcement of a criminal law of a foreign country*
 - *When is access to prospective telecommunications data permitted?*
 - *Prospective data disclosure to a foreign country*
 - *What must an AO consider when approving telecommunications data requests?*
 - *How must an authorisation be made?*
 - *Use and Disclosure of Telecommunications Data*
 - *Records and Reports for historical and prospective telecommunications data requests*
- Journalist Information Warrants
 - *Considerations*
 - *Who is authorised to issue a JIW*
- Surveillance Devices
- Control Order monitoring warrants
- Delayed Notification Search Warrants
 - *Issuing of a DNSW*
 - *When does the occupier need to be notified that their premises was searched?*

UNCLASSIFIED

Outcomes sought

At the completion of the online training program, it is the AFP's expectation that AOs who have successfully completed the training are in a position to know and understand:

- Status as a particular Authorised Officer
- Key responsibilities as an AO under relevant legislation
- Knowing where to look for further tools and assistance in meeting their obligations
- Knowing what to look for in a compliant application
- Key risks and implications of their decision-making, and
- Knowledge and awareness of reporting obligations and the Ombudsman's oversight role

Detailed summary of topics

Authorised Officers

This section refers to relevant legislation as to specific ranks or positions that may be classed as an AO and reminds officers to check they have the relevant delegation or authorisation before exercising any authority (in particular those acting in Senior Executive Service positions).

The responsibilities of an AO are set out, including to understand the requirements of relevant legislation, and being satisfied sufficient information and requirements for granting an authorisation are met in every instance.

Key risks and potential consequences of non-compliance are highlighted, including risks to admissibility of evidence and risk of legal liability.

Reporting and Commonwealth Ombudsman Inspections

This section highlights that AFP activities attract significant public and media attention, and the use of covert powers (which are given to law enforcement agencies for the purposes of combating crime and protecting our community) are the subject of a high level of examination and political and public debate.

The covert nature of these powers means independent oversight of compliance with legislation is important. The Commonwealth Ombudsman provides independent oversight by conducting inspections of law enforcement records to assess compliance with the Acts and determine whether adequate processes, procedures and training are in place to ensure legislative compliance.

An overview of the Commonwealth Ombudsman's independent oversight role and inspection process is provided, along with annual reporting requirements. The AFP's transparent approach to inspections - to identify and self-disclose any issues that arise from use of investigative powers – is noted with reference to the dedicated team to address and improve compliance practices.

Controlled Operations

A controlled operation is undertaken for the purpose of obtaining evidence that may lead to the prosecution of a person for a serious offence, and involves a law enforcement officer, or other person, participating in conduct that would constitute a criminal offence.

The AFP has developed a suite of detailed guidance to support AOs in ensuring compliance with the requirements of the controlled operations regime. The TID Handbook and training program provide guidance to AOs in respect of their obligations when approving or varying controlled operations. A number of 'common issues' identified through previous Ombudsman inspections are also included to assist AOs.

UNCLASSIFIED

Telecommunications Interception Warrants

Consistent with the topics outlined above, the TID Handbook and training program provide guidance to AOs in respect of their obligations in relation to telecommunications interception warrants. The TIA Act has a comprehensive regime in respect of notifications, documents that need to be used for evidentiary purposes and reporting obligations.

The scope, threshold and type of warrants available under the TIA Act are set out, along with the functions that are performed by an AFP AO.

[In the training program, there are a series of questions which must be answered]

Stored Communications and Preservation Notices

Stored communications are communications that have already occurred and are stored on a carrier's systems. Where the AFP wishes to gain access to stored communications held by a telecommunications carrier then the AFP must apply to an external issuing authority (AAT member or eligible Judge) for a warrant to access stored communications. Before a warrant is issued, the AFP may provide written notice to a carrier to preserve stored communications, to prevent a carrier from destroying the communication before it can be accessed under a warrant.

Consistent with the topics outlined above, the TID Handbook and training program provide guidance to AOs in respect of their obligations in relation to preserving and accessing stored communications. It details the differing requirements between domestic and foreign requests. In respect of foreign requests, it provides guidance on when a mutual assistance request will be required.

Data Authorisations

Chapter 4 of the TIA Act outlines how enforcement agencies (including AFP) may access metadata held by a telecommunications carrier.

Consistent with the topics outlined above, the TID Handbook and training program provide guidance to AOs on internally issued authorisations which enable carriers to lawfully disclose information or documents, including metadata to the agency.

It covers both historic and prospective data authorisations under the TIA Act and the scope and limitations of each provision (including in respect of both domestic and foreign requests), use and disclosure of information obtained and recording and reporting requirements. Importantly, the Handbook identifies restrictions, for example circumstances where a Journalist Information Warrant (JIW) **MUST** be applied for before any subsequent authorisations under ss178, 178A, 179 or 180 are applied for. This is covered in the training program on JIWs (see further detail on JIWs below).

[In the training program, there are a series of questions which must be answered]

Journalist Information Warrants and Authorisations

A Journalist Information Warrant (JIW) is required to permit access to telecommunications data relating to a person (or employer of a person) who is reasonably believed to be working in a professional capacity as a journalist, where a purpose for making the authorisation is to identify another person who is reasonably believed to be a journalist's source of information.

Both the TID Handbook and training program provide clear and detailed guidance in relation to requirements of JIWs. It explains key features of the JIW regime (including the role of Public Interest Advocates) and making clear who in the AFP is an AO and can make a data authorisation following the obtaining of a JIW. AOs are

UNCLASSIFIED

reminded to contact the AFP Special Projects Registrar and TID Statutory Procedures Team (and AFP Legal where appropriate) before an application for a JIW is made, and links are provided to information sheets and relevant internal guidance documents.

[In the training program, there are a series of questions which must be answered]

Surveillance Devices - warrants

The TID Handbook and training program provide guidance to AOs in respect of their obligations in relation to surveillance device warrants. The SD Act has a comprehensive regime in respect of notifications, documents that need to be used for evidentiary purposes and reporting obligations.

The scope, threshold and type of warrants available under the SD Act are set out, along with the functions that are performed by an AFP AO.

[In the training program, there are a series of questions which must be answered]

Control Order Monitoring Warrants

If a person is subject to an interim or confirmed control order made under Division 104 of the *Criminal Code*, for purposes connecting with monitoring the person's compliance with the control order, warrants can be obtained under the TIA Act and SD Act.

The TID Handbook and training program provide guidance to AOs in respect of their obligations in relation to these types of warrants. The scope, threshold and type of warrants available under the TIA Act and SD Act are set out, along with the functions that are performed by an AFP AO.

Delayed Notification Search Warrants

Consistent with the topics outlined above, the TID Handbook and training program provide guidance to AOs in respect of their obligations when internally authorising the making of an application to an eligible issuing officer under this regime.