Australian Government

Department of Infrastructure, Transport,
Regional Development and Local Government

GUIDANCE PAPER:
Preparing a TRANSPORT SECURITY PROGRAM

For operators of Security Controlled Airports

This guidance material details important information that you should consider when preparing your Transport Security Program.

Disclaimer: This document is designed to provide general guidance to airport operators, operating under arrangements according to the Aviation Transport Security Act 2004 (the ATSA) and Aviation Transport Security Regulations 2005 (the ATSR) in developing Transport Security Programs (TSPs) for submission to the Secretary of the Department of Infrastructure, Transport, Regional Development and Local Government (The Department) for approval.
This guide should not be used by airport operators as a substitute for obtaining independent professional advice (including legal advice) regarding their TSP and the TSP's compliance with the requirements of the ATSA and the ATSR. This document is subject to change. the Department is not responsible for the consequence of the use of any outdated version of this guide.

Table of Contents

PREFACE

This guide has been developed for use in the preparation of TSPs. It is designed to provide general guidance for airport operators to meet their TSP obligations under the *Aviation Transport Security Act 2004* (ATSA) and *Aviation Transport Security Regulations 2005* (ATSR).

Division 4 of Part 2 of the ATSA sets out the general requirements for TSPs for aviation industry participants (AIPs). Section 16 of the ATSA describes the required content of TSPs and section 17 describes the required form of TSPs. Additional content and form requirements which apply to airport operators are outlined in Part 2 of the ATSR, especially Division 2.2 – Operators of security controlled airports.

ABBREVIATIONS

The following abbreviations are used in this document:

AIP	(Aviation Industry Participant)
ANA	(*Air Navigation Act 1920*)
ASC	(Airport Security Committee)
ASIC	(Aviation Security Identification Card)
ATSA	(*Aviation Transport Security Act 2004*)
ATSR or **Reg.**	(*Aviation Transport Security Regulations 2005*)
CERHOS	(Ceremonies & Hospitality Branch, Dept of Prime Minister & Cabinet)
CBS	(Checked Baggage Screening)
DITRDLG or *The Department*	(Department of Infrastructure, Transport, Regional Development and Local Government)
ETD	(Explosive Trace Detection)
MTES	(*Methods, Techniques & Equipment to be used for Screening*)
OTS	(Office of Transport Security)
SCO	(Security Contact Officer)
RACA	(Regulated Air Cargo Agent)
TSP	(Transport Security Program)
VIC	(Visitor Identification Card)

BACKGROUND

The ATSA and ATSR came into force on 10 March 2005, replacing Parts 3 and 3A of the ANA, and Part 7 of the *Air Navigation Regulations 1947*. The ATSA established

a new regulatory framework to safeguard against unlawful interference with aviation, and the ATSR provides the details necessary for the ATSA to operate as intended.

The changes in the law strengthened Australian aviation transport security systems and enabled a broader and more inclusive approach to aviation security. The ATSA and ATSR emphasise the need for AIPs to demonstrate a fuller awareness of their general responsibility to contribute to the maintenance of aviation security: ATSA s.16(1)(a). The ANA imposed a large number of prescriptive measures, while the ATSA and ATSR focus more on outcomes.

An Aviation Industry Participant's TSP should detail measures and procedures for aviation security based on an AIP's assessment of its own risk environment.

Note: As a result of amendments to the ATSR, airside facility operators are no longer required to have a TSP.

CONTENT AND FORM REQUIREMENTS FOR TSPs

ATSA s.16(1) states that a TSP for an AIP (which includes an airport operator) must demonstrate that the participant:

- is aware of the participant's general responsibility to contribute to the maintenance of aviation security; and
- has developed an integrated, responsible and proactive approach to managing aviation security; and
- is aware of, and has the capacity to meet, the specific obligations imposed on the participant under the ATSA and the ATSR; and
- has taken into account relevant features of the participant's operation in developing activities and strategies for managing aviation security.

ATSA s.16(2) states that a TSP for an AIP must set out the following:

- how the participant will manage and co-ordinate aviation security activities within the participant's operation (*you should consider what communication and control procedures are in place; whether the roles and specific tasks of AIP management staff are defined clearly; whether the communication and control arrangements appear likely to enhance security measures; and whether there is sufficiently broad representation on relevant Airport Security Committees (ASCs)*); and
- how the participant will co-ordinate the management of aviation security with other parties (including Commonwealth agencies) who have responsibilities for, or are connected with, aviation (*consider whether the Terms of Reference for the ASC are described within the TSP; other government agencies are involved with security; the duties of these agencies are clearly outlined in the TSP; which management positions are represented on the ASC; and which position has overall responsibility for management of the TSP*);
- the technology, equipment and procedures to be used by the participant to maintain aviation security (*have standard operating procedures been formulated and implemented?*);

- how the participant will respond to aviation security incidents (*measures may include communication and control, implementation of security measures, public safety and continuity of essential operations. Are the response roles of other agencies clearly described?*);
- the practices and procedures to be used by the participant to protect security compliance information (*you should consider document (paper and electronic) control/protection, identification and classification, access control, email classifications, and document distribution and destruction*);
- the other AIPs who are covered by, or operating under, the program (*are there effective communication and control procedures to ensure all AIPs covered under the TSP can implement their responsibilities under the TSP?*);
- the consultation that was undertaken with other AIPs who are covered by, or operating under, the program.

Further, ATSA s.17 provides that the TSP must be in writing and prepared in accordance with any requirements set out in the ATSR. When reviewing a TSP from a security controlled airport for approval, the Department will be assessing whether, overall, the TSP satisfies the requirements of ATSA s.16(1) and (2) and the ATSR, and that there is sufficient evidence that the participant has undertaken the informative, consultative, planning and investigatory processes inherent in those requirements. Under the ATSA, if the Secretary is not satisfied that the TSP adequately addresses the relevant requirements, the Secretary must refuse to approve the TSP (s.19(2)).

Although participants are required to comply with all sections of the ATSA and ATSR that apply to them, their TSPs need only contain the information that the ATSA and the ATSR require to be set out in a TSP. TSPs should not contain measures and procedures that are inconsistent with the ATSA or ATSR.

The body of the TSP is not intended to be an operations manual describing how to do things in minute detail, but rather an outline of an AIP's security risk environment, and what things (ie. measures and procedures) they will do to deter and detect unlawful interference with aviation. However, TSPs submitted to the Department often do not contain a level of information likely to be sufficient for the Secretary to be satisfied that the AIP meets all that is required under the ATSA, particularly ATSA s. 16. This is particularly the case where reference has been made to other documents, but those documents are not provided with the TSP. Such issues might be overcome through the attachments of the relevant document, or alternatively through greater detail in the TSP, without necessarily attaching the separate document (see 'TSP Accompanying Documents' below).

The TSP must meet the form and content requirements as stipulated by the ATSA and ATSR. For example, where a Regulation says the TSP 'must set out' certain measures and procedures, the TSP must state or explain its measures and procedures systematically within the body of the TSP. The participant may wish to provide more detailed measures and procedures in an accompanying document, as additional information, but must still meet the basic requirements as set out in the Regulation.

PREPARING A TRANSPORT SECURITY PROGRAM

When preparing a TSP, you should consider:

- Whether you have individually tailored the TSP to take account of your airport's specific local risks and the scope of your operations, with security measures and procedures reflecting risk mitigation strategies identified from your assessment of your security risk; and

- Whether the TSP meets the content and form requirements of the ATSA and ATSR.

The Department recognises that each Regulation relating to TSPs may be open to interpretation in the context of the details of each participant's operation. It also recognises that the way in which airport operators will meet their legislative obligations with respect to TSPs will be relative to their unique operations.

When the Department assesses your TSP, it will:

- Identify any areas with missing data;

- Ensure accuracy, consistency and standard of spelling, grammar and data;

- Assess TSP compliance/non-compliance with the ATSA and ATSR.

General Guidance

- TSPs should always use correct terminology. It should be internally consistent throughout the TSP and between maps and text; terminology should be consistent with the legislation.

- Terminology such as 'airside', 'security restricted area' (SRA), and 'sterile area' is correct. TSPs may state that the 'airside security zone' equals the security restricted area, and that 'landside security zone' equals the sterile area.

- Terms like 'security restricted zone', 'security cleared zone', 'non-airside' and 'non-landside' should not be used. Also, the terminology of former legislation should be avoided.

- If sites such as the Air Traffic Control Tower and the fuel storage facility are acknowledged as landside security zones, the TSP must outline the mechanisms for consultation with the owners of those facilities.

- Use of the correct tense is important. The TSP should be in the present tense, describing the measures that are currently in place, not near future proposals

- However, near future proposals are acceptable in the following contexts:

- the future proposal will complement existing measures and procedures;

- to satisfy Reg. 2.16(2);

- where a TSP for an airport operator addresses proposed airside or landside security zones; or

- in relation to TSPs of airport operators: Adelaide, Brisbane, Melbourne, Perth, Sydney, Cairns, Canberra, Coolangatta and Darwin, airports are currently required to have checked baggage screening capability. From 1 August 2007, these airports, as well as the Alice Springs and Hobart airports, will need to have checked baggage screening. Therefore, future proposals regarding checked baggage screening being performed from 1 August 2007 by such airport operators would also be acceptable.

- TSPs should not state timeframes that contradict those which are set out in relevant legislation.

- TSPs should focus on the AIP's own responsibilities, and not cite other AIPs as having responsibility for certain measures or procedures.

- If referring to security measures carried out by other AIPs with whom you interact, you should be aware that such references do not bind that other participant; they should be the subject of consultation and are not a substitute for the obligations of the TSP holder under the ATSA and ATSR.

- As highlighted below under 'TSP Objective', the TSP should reflect the security risk assessment, and vice versa. The body of the TSP could bring to light an issue that should be included in the risk assessment.

- If the Regulations call for 'measures' and 'procedures', then the TSP must spell out nothing less than measures and procedures. If the Regulations call for measures to 'deter and detect', then details of the measures for deterrence and detection must be set out in the TSP.

- Where AIPs have additional plans (such as ASIC plans, CBS plans, airport emergency plans etc.), which comprehensively address the content and form requirements of specific regulations, the AIP may attach such plans to the TSP, as accompanying documents, to meet those regulatory requirements. However, AIPs should be aware that if additional plans are attached they will form part of the TSP. Please refer to the section on "TSP Accompanying Documents" for more details.

- The TSP must reflect current regulatory reality, and not an anticipated reality. AIPs must complete their TSPs by using the current ATSA and ATSR found at http://www.comlaw.gov.au Industry will be advised of any regulatory changes.

- Where the TSP discusses incident reporting, the information must be clear (citing to whom reporting will be made), and cannot contradict the Notice About How Incident Reports are to be Made.

- If the airport operator has satisfied Reg. 2.16(2), and would like to implement additional measures as part of their TSP, the airport operator should note that it will be held accountable for all of the additional measures included in their TSPs. If the airport operator fails to meet those additional measures identified in the implementation timetable, the airport operator must have a reasonable excuse to avoid enforcement action.

- If the airport operator has not satisfied Reg. 2.16(2), the airport operator is to identify when specific measures and procedures would be implemented. If approval of the TSP is given prior to that time, the Department will not enforce the provisions of the TSP until after the deadlines specified in the implementation timetable.

When the Department reviews a TSP, the Department will be considering and assessing whether, overall, the TSP satisfies the requirements of ATSA ss.16 and 17, and the relevant provisions of the ATSR. Under ATSA s.19, if the Secretary is not satisfied that the TSP adequately addresses the relevant requirements, the Secretary must refuse to approve the TSP. Where this is the case, the Secretary must also give the participant a written notice of the refusal.

Finally, where AIPs have recruited consultants to develop content for TSPs, you should be aware that the Department assumes that AIPs who submit TSPs for assessment have sufficient intellectual property rights to do so.

Security Classification of TSPs

Some industry participants give their TSPs security classifications that are neither national security classifications nor non-national security classifications. The Department wishes to advise airport operators that TSPs should generally be classified 'IN-CONFIDENCE'.

TSP Accompanying Documents

A distinction is drawn in the ATSR between circumstances where a TSP 'must be accompanied by a document that sets out' certain information and circumstances where a TSP 'must set out [certain information] in an accompanying document'.

The Department takes the view that there is a difference in meaning between those Regulations which provide that the TSP must be 'accompanied' by a certain document [Regs. 2.13(4), 2.13(9), 2.19], and the Regulations which provide that 'the TSP must set out, in an accompanying document, [certain information] …' [Regs. 2.10, 2.11(3), 2.21].

The Department interprets these Regulations as follows:

- Where the Regulations provide that 'the TSP must be accompanied by a document' the information provided is to be treated as a separate document from the TSP. This document is not subject to the same formal variation and revision requirements as the TSP.

- Where the Regulations provide that 'the TSP must set out, in an accompanying document, [certain information]' the information provided, although in a separate document, is to be treated as constituting part of the TSP. This document is subject to the same formal variation and revision requirements as the TSP.

The practical effect of this distinction is that AIPs may need to consider whether the documentary material which has been provided with their TSP lodged for assessment is material that is required by the Regulations to form part of the TSP or is instead material which is separate to the TSP.

While the Department recognises that at this point in time it is not necessary for AIPs to have supplied all of the accompanying material not forming part of the TSP to the Department, the Department is aware that in a number of cases AIPs have in fact done so or intend to do so. TSP assessors have therefore been requested to consider whether any material submitted in addition or as a supplement to the TSP may in fact satisfy the requirements set out in those Regulations requiring that the TSP be 'accompanied by' a document setting out prescribed information.

Assessors have also been requested to consider any material that has been submitted to address those Regulations requiring that certain information be set out in an 'accompanying document'. In circumstances where such information has not been provided, this will be relevant to the consideration of whether the TSP can, as a matter of fact, satisfy the requirements of s.16 of the ATSA.

Finally, the Department notes that, in some circumstances, an AIP may have chosen to submit certain information by way of a separate document, rather than in the body of the TSP. The Department wishes to advise AIPs that this information will nevertheless form part of the body of the TSP for assessment purposes if it is information that must be 'set out' in the body of the TSP, in accordance with the Regulations. Any such documents, although they may be physically separate from the TSP, will also be subject to the TSP variation and revision requirements set out in the ATSA.

CONTENT OF A TSP

Scope of TSP

The TSP must cover any aviation security-related activity on the airport that is not covered by the TSP of any other AIP (Reg. 2.09).

Statement of Undertaking (ATSA s.16(1); Reg. 2.05)

Under ATSA s.16(1), AIPs have certain obligations. The TSP for an AIP must demonstrate that they:

- are aware of their general responsibility to contribute to the maintenance of aviation security (*consideration should be given to your local risk context*);

- have developed an integrated, responsible and proactive approach to managing aviation security (*the TSP should be inclusive of other AIPs where necessary*);

- are aware of, and have the capacity to meet, the specific obligations imposed on the AIP under the ATSA; and

- have taken into account relevant features of their operation in developing activities and strategies for managing aviation security (*you should consider factors including your local risk context, described within security risk assessment, inclusion of AIPs within TSP, basic security measures, remoteness of operator, risk categories*)

Also, under Reg. 2.05, a TSP must contain a 'Statement of Undertaking', signed by the participant. When the participant signs, the participant is stating that the participant believes that the TSP gives effect to the above obligations. This is not a statement that the participant will implement a TSP. An appropriate person should sign the Statement, and include it in the TSP.

You should ensure that your security risk assessment is not outdated, such that there are changes in circumstances that may change your security measures and procedures.

TSP Objective

The TSP must contain an outline of the objectives of the TSP and must be accompanied by a document which contains a local security risk context statement (this document may be attached as an appendix (Reg. 2.10(a))).

The local risk context statement is to include a statement outlining your local security risk context, including consideration of location, seasonal and operational factors. Mention could be made of previous threats, incidents, criminal activity or vandalism, relating to international, domestic, cargo and/or general aviation. If you feel that no seasonal factors have security implications for your operations, a brief note to that effect should suffice.

The accompanying document must also include (Reg. 2.10(b)-(c)):

- a list of general threats and generic security risk events to people, assets, infrastructure and operations; and

- an outline of the people, assets, infrastructure and operations that need to be protected.

The TSP should reflect the security risk assessment, and vice versa. If the security risk assessment reveals a significant body of threat affecting the AIP, the TSP should spell out measures and procedures appropriate to counter that threat. Similarly, a small regional AIP, situated far from large population centres, may have a much smaller risk environment. The measures and procedures cited in its TSP should also mirror that environment. The TSP should always specify satisfactory mitigating strategies to reflect the AIP's current security risk assessment.

AIPs are not required by legislation to complete a full security risk assessment, nor to attach a risk assessment plan to their TSP. The Regulations only require participants to set out, by way of an accompanying document 'a statement outlining the local security risk context of the [AIP] including consideration of its location and seasonal and operational factors'.

An airport operator's local security risk context statement should be substantial, and should provide a benchmark for the level of security and the kinds of security measures and procedures proposed. The information set out in the accompanying document (which includes the local security risk context statement) should be clear and thorough, however, probably not at the level of detail required in a full risk assessment plan.

It may be appropriate for an operator to adapt the executive summary of its risk assessment plan and utilise it for the local security risk context statement.

PROCEDURES FOR MANAGING SECURITY

Security Management

(Security Contact Officer (SCO), staff, other agencies/contractors, training, awareness)

Under Reg. 2.11(1), TSPs for airport operators must set out the procedures for managing security at the airport, including:

a) organisational structures and security management arrangements; and

b) the roles and responsibilities of security contact officers, security staff, contractors and responding agencies; and

c) the roles and responsibilities of other staff who have been assigned security duties and responsibilities; and

d) the roles and responsibilities of other Commonwealth, State and Territory agencies, and local authorities, with security duties at the airport.

AIPs must include their organisational structures and security management arrangements in their TSPs to show where their security functions are within their organisation. The entire organisational structure of the operator does not need to be included; TSPs should focus on the main security function within the operator. Operators may include a diagram to demonstrate this. You should ensure that the TSP contains contact details for yourself (both during hours and after hours) and the SCO (in this context, there must be a 24-hour security contact number) (Reg. 2.13(4)).

TSPs must include a description of the roles and responsibilities of SCOs, security staff, contractors and responding agencies. An SCO should be the first point of contact for security matters. The roles and responsibilities of the SCO should include:

- facilitating the development, implementation, review and maintenance of the TSP; and

- undertaking liaison with other AIPs and responding agencies (eg, Police, Fire Brigade, Emergency Services etc) on aviation security matters.

A comprehensive description of the SCO's roles and responsibilities should be provided in the TSP, as well as any responsibilities delegated to others within the organisation (Reg.2.11(1)(b))(see Reg. 2.02 for SCO roles and responsibilities).

TSPs must include a description of other persons (other than the SCO and security staff) who have been assigned security duties and responsibilities (Reg 2.22(2)). Employees should be specified by position, and not by their names. Contractors' positions must be included. The duties and responsibilities of such employees, contractors and other persons should be described, in addition to the knowledge, skills and experience required for the security-related aspects of their positions and the training or qualifications that satisfy the requirements of the position (Reg. 2.22(3)).

TSPs must also include a description of the role and responsibilities of other Commonwealth, State or Territory agencies and local authorities that have security duties at the airport (eg. local councils, State or Territory Police, government agencies or statutory authorities). The operator should outline how these duties relate to the TSP, and demonstrate the processes in place to call on these authorities during a heightened security alert (Reg.2.11(1)(d)).

TSPs should contain descriptions of the training that an SCO would be required to undertake, as well as criteria for their selection (Reg. 2.22(1)). Any aviation security training programs provided to others with security roles should be described.

To maintain a robust security culture in the aviation industry, AIPs should conduct security awareness training to meet the requirements of Regs. 2.21(2)(e) and 2.22(4), which highlight the importance of alertness to security threats, and responsibility to report incidents. This security awareness training should be demonstrated in the TSP: the training course content is not required, an outline of the type of training will suffice.

Consultation

TSPs need to reflect an integrated, coordinated and proactive approach to aviation security. Consultation between participants is a significant practical step in ensuring this outcome.

Inclusion with TSPs of evidence that such consultation has occurred will provide OTS with an assurance that participants have consulted with other relevant AIPs in relation to those parts of the TSP that affect them. This does not have to be advice of agreement between the parties, but is illustrative of appropriate sharing of information between participants.

To ensure consistency within and between different types of AIPs, examples of evidence might include:

- minutes from a meeting of stakeholders (eg the Airport Security Committee)
- registered mail receipt evidencing information being provided
- evidence of consultation with representative bodies (eg BARA)
- signed letters from individual AIPs confirming consultation
- proof of emailing of relevant material

Security of Information

ATSA s.16(2)(e) requires that a TSP must set out the practices and procedures to be used by the AIP to protect security compliance information. In addition, Reg. 2.11(4) requires that a TSP must set out measures to ensure that the TSP and other security information are protected against unauthorised access, amendment and disclosure. The Department suggests that together with measures and procedures for protecting the TSP from unauthorised access (eg. safe storage of hard and electronic copies etc.), airport operators should describe how relevant people who have access to the airport are made aware of their security obligations. It should be noted that a person can be prosecuted for breaching Reg. 2.06. In addition, airport operators need to consider a range of circumstances when information might, in fact, need to be shared. This could include external auditors scrutinising the material.

Operators should outline procedures for controlling and protecting the TSP and other security information, including compliance information. Such measures could include:

- Safe storage of the TSP, for both hard and electronic copies of the document, such as computer security policies;
- Reference to the security classification of the document;
- Who is authorised to access the information in the security risk assessment and TSP;
- Who is authorised to issue copies of the TSP;
- Who is authorised to amend the TSP;
- Measures for returning and destroying outdated TSP documentation (both hard and electronic copies); and
- Measures to record the issue of copies of the TSP (both hard and electronic copies).

An example format for recording the issue of TSP copies is provided below.

TSP DISTRIBUTION RECORD			
Copy No.	**Held By**	**Organisation**	**Contact Details**
1	General Manager	ABC Flying	0400 111 222
2	Station Commander	DEF Police Station	(02) 4235 1111
3	Office of Transport Security (OTS)	Department of Infrastructure, Transport, Regional Development & Local Government	

PROCEDURES FOR QUALITY CONTROL

Procedures

A TSP must set out quality control measures, including a schedule of, and procedures for, internal security program audits and reviews. This is required under Reg. 2.12.

Recommendation VIII of the Wheeler Review of Airport Security and Policing was that TSPs have a more frequent system of reporting, ensuring airports regularly review their own security gaps and weaknesses, and document the measures being taken to address them. The requirement at Reg. 2.12(1) is adequate for the time being. However, the Department suggests that airports consider Wheeler Recommendation VIII when drafting this section of their TSPs.

Audits

An audit is defined in Reg. 2.01(2) as an examination by an AIP of security measures under their TSP to find out whether the measures have been correctly implemented. An audit should involve an in-depth examination of all aspects of an AIP's TSP, to determine whether they are being implemented continually and to an appropriate standard.

Audits should be undertaken regularly, in accordance with clearly defined procedures and parameters. You should ensure that the TSP (Reg.2.12(1)(a)-(b)) includes:

- a schedule of audits; and
- the process for selecting an auditor.

Information about the AIP's schedule of security audits may include frequency of the audits, the types of audits undertaken, and the staff involved. They could be regular scheduled audits, unscheduled spot audits, internal or external.

The TSP should show that the AIP has taken into account the potential for conflict of interest if internal auditors are used. It is preferred that audits be conducted by external, independent persons. However, if this is not possible, a person from within the organisation may be selected, provided they are not directly responsible for the implementation of the TSP.

Reviews

A review of an AIP's TSP is defined in Reg. 2.01(2) as an evaluation by the participant of security measures or procedures under its TSP to find out whether the measures and procedures are adequate.

The aim of the review is to assess how effective the current TSP is in meeting the ATSA's objectives. Reviews should be undertaken regularly, with clearly defined procedures and parameters. You should ensure that the TSP includes a procedure for consultation to be undertaken to ensure security measures and procedures are adequate and the TSP is being appropriately implemented (Reg. 2.12(1)(c)).

The AIP's review procedures should also describe the circumstances that will require a review of the TSP (eg a change in the security environment), including those surrounding an occurrence of an aviation security incident (Reg. 2.12(1)(d)). The review procedures should include adequate consultation with other AIPs, recognising that security outcomes are reached through the cooperation of all participants.

Audit and Review Records

It is mandatory that the records of each audit are kept for at least seven years after the audit is completed, and that the records of each TSP review are kept for at least three years after the review is completed (Reg. 2.12(2)).

DETAILS OF AIP's NAME AND OPERATIONS

Operational details

Description of Airport

Under Reg. 2.13(1), in addition to maps showing the airport boundaries and security zones, the TSP must set out:

a) the name of the airport;

b) its geographic location, including a reference to the closest population centre;

c) the types of aircraft operations that operate to and from the airport, including regular public transport, cargo, general aviation and joint-user facilities and other significant operations that may require security considerations;

d) the size of the airport (*eg. size in hectares*);

e) a description of significant features affecting the security of the airport perimeter, such as waterways or residential areas (*proximity of housing*);

f) a description of the airside and landside operations for which the airport operator has responsibility;

g) the hours during which the airport normally operates;

h) whether access into landside and airside areas and zones and internal security of such areas and zones is controlled at all times or not (*consideration should be given to mobile or foot patrols. Is the fencing likely to achieve the desired security outcomes as described within the security risk assessment?*); and

i) details of procedures for security outside normal hours of operation (*consideration should be given to the totality of all access control arrangements, not just the existence or absence of a particular access control measure in isolation*).

Other AIPs within the Airport

Under Reg. 2.13(2), an airport TSP must identify all AIPs that have a facility at, or are located within, the airport, and are covered by their TSP or another AIP's TSP.

> *Note: This Regulation, in most cases, will no longer be relevant. An example which may still have relevance is an airline which also operates as a RACA. In most cases, an airport operator may respond to this requirement with 'N/A – there are no AIPs that have a facility at, or are located at the airport that, although required to have a TSP, are covered by the airport or another operator's TSP'.*

If the airport TSP covers another AIP that is required to have a TSP or be covered by the airport TSP, the TSP must list the contact details for each such participant. Where the TSP follows the Department's "*Template for writing a Transport Security Program (TSP) - Airport Operators*" format, this may be included as **Appendix E)**.

Airport Operator's Contact Details

Under Reg. 2.13(4), the TSP for an airport operator must be accompanied by a document that sets out the following:

a) airport operator's name;

b) name of its chief executive officer or manager;

c) airport operator's mailing address, if different to the airport's location;

d) airport operator's fax number;

e) airport operator's contact telephone number, including an after-hours number;

f) alternative contact person and number; and

g) name of the security contact officer and his or her business phone number, fax number, email address and a 24-hour security contact number.

Maintaining Contact with all AIPs within the Airport

Reg. 2.13(8) provides that an airport operator's TSP must require the airport operator to maintain a system enabling all AIPs with a facility at, or located within, the airport to be contacted if an aviation security incident occurs. The TSP should outline the procedures for contacting those AIPs in the event of an aviation security incident. It is recommended that operators also include procedures for ensuring that relevant participants can be contacted in a timely manner in case of an aviation security incident.

Security Zones

> *Please note that in relation to airport security zones, airport operators must ensure that their TSP is not inconsistent with Divisions 3.2, 3.3 and 3.4 of the ATSR. If your airport is a 'designated airport' (an airport that requires counter-terrorist first response function), your TSP must also not be inconsistent with Division 3.5 of the ATSR.*[1]

If a new airside or landside security zone is to be established at the airport, you must, under Reg. 2.14(1), set out in your TSP:

a) the purpose of establishing the zone;

b) the proposed boundaries of the zone (*determine whether signposting is at visible distances apart and signage indicating an airside area/security zone is clearly identifiable by the public*);

c) if applicable, the period when, or the circumstances in which, the zone will be in force; and

d) the name or position of the person or persons responsible for security measures in relation to the zone.

Under Reg. 2.14(2), your TSP must also set out security measures and procedures to monitor and control access to landside and airside security zones, including measures to detect and deter unauthorised access to these zones.

Any current airside and landside security zones (as laid out in the *Notice Establishing Airside and Landside Security Zones*, effective since 10 March 2005), must be described in terms of Reg. 2.14(1).

You should provide a map clearly showing control of all access points and any airside or landside security zones within the security controlled airport. Where the TSP follows the Department's "*Template for writing a Transport Security Program (TSP) - Airport Operators*", the map may be included as **Appendix G** to the TSP.

Note: Reg 2.09 provides that your TSP must cover any aviation-security related activity on the airport that is not covered by the TSP of any other aviation industry participant. The Department takes the view that it is not appropriate for the same aviation-security related activity to be covered by two AIPs' TSPs. For example, it is appropriate for Air Services Australia's TSP to deal with security related activities concerning the air traffic control tower. If Air Services Australia's TSP deals with those activities, any conflicting provisions in your TSP dealing with activities concerning the tower should be removed. Your TSP may need to be varied if it deals with security-related activities concerning the air traffic control tower. However, any consultation that *has* taken place should be indicated in your TSP.

[1] Note: the following airports are designated airports - Adelaide Airport, Alice Springs Airport, Brisbane Airport, Cairns Airport, Canberra Airport, Coolangatta Airport, Darwin Airport, Hobart Airport, Melbourne Airport, Perth Airport and Sydney Airport.

Forms of Maps

Under Reg. 2.15, the airport operator's TSP must include a map which clearly delineates the airside and landside areas and any airside security zones and landside security zones for the airport. This map should be attached to the TSP. Where the TSP follows the Department's "*Template for writing a Transport Security Program (TSP) - Airport Operators*", the map may be included as **Appendix F**.

The map must:

a) have a linear scale;

b) show a north point;

c) show the latitude and longitude of the airport;

d) be in black and white only, with limited shading;

e) be a clear and light featured depiction of the airport and its airside and landside areas;

f) show the boundary of the security controlled airport.

For the purpose of gazetting the boundaries of a security controlled airport (ATSA s.28), multiple A4-sized maps aggregating to cover the entire boundary of the security controlled airport (including the airside area) should be provided. The map(s) must adhere to points a) to f) above. In addition, AIPs may apply 12% greyscale shading to delineate airside areas. While this is not mandatory, it is recommended by the Department for the purposes of satisfying Reg. 2.15(e). As the map(s) is for gazettal, it must not show any security zones.

In addition to the requirement for a map of the security controlled airport for gazettal, Regs 2.15(2), (3) and (4) require several other maps to be included in the TSP. The additional maps do not need to be detailed plans. General outlines of areas for clarity of security responsibilities will suffice (see Reg. 3.02 for types of landside security zones).

Maps of airside/landside security zones should be of a scale to ensure that zones are clearly able to be distinguished, including clear illustrations of whether buildings are within or outside of security zones. For the purpose of providing maps with the TSP (as required by Reg. 2.15), there are no size restrictions when submitting the TSP electronically, provided that the boundaries on the electronic version of the maps are clear.

Maps should always make sense. In the past, some airport operators have submitted maps that are not clear. Legends in previously submitted maps have depicted airside as white, while the map itself shows both airside and landside as white. The security controlled airport boundary on some maps is a challenge for the eye, becoming lost among terminal buildings and car parks. A hangar that shows as partly airside, partly landside should be accompanied by an explanation. If not, you should question this. Following the production of a new map version, any old dates surviving the change create ambiguity; airport operators should remove them.

Aircraft parking positions

Under Reg. 2.15(2), your TSP must include a map of the location of regular and isolated aircraft parking positions. This map should be attached to the TSP. Where the TSP follows the Department's "*Template for writing a Transport Security Program (TSP) - Airport Operators*", the map may be included as **Appendix H**. Isolated parking positions, for example, may be used by aircraft that have been the subject of unlawful interference. Ideally, the designated isolated parking position should be a reasonable distance from the passenger terminal and facilities such as fuel farms. Those assessing your TSP will have these issues in mind.

Sterile areas and screening points

If a screened air service operates from your airport, Reg. 2.15(3) requires that the TSP must include a map of the airport terminal(s) showing the location of all screening points and landside security zones including sterile areas. This map should be attached to the TSP. Where the TSP follows the Department's "*Template for writing a Transport Security Program (TSP) - Airport Operators*", the map may be included as **Appendix I**.

Aprons at screened airports

If a screened air service operates from your airport, Reg. 2.15(4) requires that the TSP must include a description and map of the apron(s) for the purposes of Reg. 4.02(3). This map should be attached to the TSP. Where the TSP follows the Department's "*Template for writing a Transport Security Program (TSP) - Airport Operators*", the map may be included as **Appendix J**.

These maps do not need to show detailed plans. General outlines of terminal areas for clarity of security responsibilities will suffice.

Physical Security and Access Control

> *Please note that in relation to physical security and access control, airport operators must ensure that the TSP is not inconsistent with Divisions 3.2, 3.3 and 3.4 of the Regulations.*

Although the airport operator may have general security responsibility for the entirety of the security controlled airport, more specific access control and physical security measures and procedures are the responsibility of the leaseholder if they are required under the legislation to have a TSP. In the case of airport terminals, the airport operator may wish to outline, under the physical security and access control section of their TSP, those parts of airport terminals that are covered by the TSP of another AIP.

The TSP for an airport operator must set out the security measures and procedures to be used within the airport to control access at the airport, including specific measures to deter and detect unauthorised access to the airside area, and any airside security zones and landside security zones. Access control arrangements may include photographic identification systems for authorised access, vehicle inspection and entry arrangements, doors and gates, and assets secured by padlocks or coded access arrangements.

Under Reg. 2.16(1)(a), the TSP must set out the security measures and procedures to control access at the airport, and maintain the integrity of access control systems. These could include, for example:

- airside access permit system, ASICs, VICs, Airside Driving Authorities;
- computerised systems;
- regular inspection of gates/controlled doors

Under Reg. 2.16(1)(b), (c) and (d), the TSP must set out security measures and procedures to deter and detect unauthorised access into the airside area, and airside and landside security zones by people, aircraft, vehicles or things.

Examples of security measures and procedures in this context could include:

- security/safety street lighting;
- fencing;
- refuelling facilities – fencing/locks, etc;
- control of access to airside through computerised ID system;
- regular inspection/patrols by airport staff/security guards;
- appropriate signage; and
- securing of vehicles.

Under Reg. 2.16(1)(e), the TSP must set out the security measures and procedures to be applied to unattended aircraft. Although primary responsibility for unattended aircraft will lie with the aircraft operator, airport operators' security measures and procedures must make reference to unattended aircraft. Such measures and procedures could include training provided to staff so they are aware of the requirement to report to their SCO or supervisor of any unattended aircraft. Measures could also include procedures for identifying unattended aircraft, who has responsibility for this; procedures for reporting to the SCO, the aircraft operator, and the Department; and procedures for securing an aircraft found to be unattended.

Under Reg. 2.16(1)(f) and (g), your TSP must set out security measures and procedures to assess, identify and respond to unknown substances; and investigate, secure and remove unattended or suspect vehicles, aircraft or things, including baggage and cargo.

Examples of security measures and procedures in this context could include:

- regular inspection/patrols by airport staff/security guards;
- isolation of an area by security staff, once a suspicious item is identified;
- notification of security contact officer; and
- notification of local authorities.

Under Reg. 2.16(1)(f), operators are not required to have staff trained to identify substances etc through analysis or other scientific means or to physically handle these items. Rather, it is the intention that operators and their staff are able to determine that an item is unusual or potentially dangerous. Subsequently, they should know how to inform and request the response of specialist agencies such as the fire brigade or Law enforcement authorities and to minimise access to items by other people.

Under Reg. 2.16(1)(h), your TSP must set out security measures and procedures to ensure the security of passwords, keys and key lists, electronic access cards and other security privileges.

Examples of security measures and procedures in this context could include:

- airport key register;
- electronic access control systems;
- master key system on locks and padlocks;
- changing codes when employees quit their jobs; and
- staff signing an undertaking of confidentiality.

Under Reg. 2.16(2), your TSP must specify which measures and procedures have already been implemented, and include a timetable for implementing measures and procedures not yet implemented. (Where the TSP follows the Department's "*Template for writing a Transport Security Program (TSP) - Airport Operators*", the timetable may be attached to the TSP as **Appendix K**).

Screening and Clearing

> *Please note that in relation to screening and clearing, airport operators must ensure that their TSP is not inconsistent with Divisions 4.1 (in particular Reg.4.39) and 5.3 of the Regulations.*

Under Reg. 2.17(1), airports with screened air services must set out in their TSP:

a) measures, equipment and procedures to carry out screening and clearing of persons and baggage; and

b) the names of the screening authorities that will undertake those functions.

If a screened air service does not operate from the airport, the TSP may state 'N/A – screening is not required at this airport under ATSA/ATSR'.

Measures and procedures set out in the TSP for screening and clearing of persons and baggage must include:

a) the locations where screening is undertaken;

b) details of the screening equipment used;

c) details of the persons who operate the equipment;

d) procedures to treat suspect passengers or carry-on baggage;

e) measures and procedures to control the movement of passengers;

f) procedures for handling and screening transit passengers from inbound international flights at their first Australian port of call;

g) measures to ensure that non-screened passengers on arriving aircraft (eg. small GA aircraft) do not mix or interfere with screened passengers;

h) measures and procedures to handle:

   i. diplomats and other VIPs;

   ii. government couriers and diplomatic bags;

   iii. passengers with reduced mobility or a medical condition;

   iv. persons in custody;

   v. suspect behaviour by a passenger;

   vi. transit passengers;

i) measures and procedures to follow sterile area breaches, including post-breach recovery plans (reg.2.17(2)).

Regulations covered by the MTES

Screening measures and procedures must comply with the applicable standards, as outlined in the document *Methods, Techniques and Equipment to be used for Screening*, which the Secretary of the Department may specify by written notice (Reg. 4.17). Many airport operators choose to articulate their screening measures and procedures by writing "As per the MTES", when completing a TSP. This can be problematic because not all Regulations are covered in the MTES. However, the following Regulations are indeed covered by the MTES. Airport operators may cite in their TSPs "As per Part x of the MTES" for the following Regulations:

Reg. 2.17(2)(b) – As per Part 2 of the MTES

Reg. 2.17(2)(c) – As per Parts 2, 3 & 7 of the MTES

Reg. 2.17(2)(e) – As per Part 2 of the MTES

Reg. 2.17(2)(h)(ii) – As per Part 2 of the MTES

Reg. 2.17(2)(h)(iii) – As per Part 2 of the MTES

Reg. 2.18(1)(a)(ii) – As per Part 6 of the MTES

Reg. 2.18(1)(a)(iii) – As per Part 6 of the MTES

Reg. 2.18(1)(d) – As per Part 6 of the MTES

Regulations not covered by the MTES

Airport operators will need to spell out their measures and procedures, in their TSPs, for the following Regulations:

Reg. 2.17(2)(a)

Reg. 2.17(2)(f)

Reg. 2.17(2)(g)

Reg. 2.17(2)(h)(iv)

Reg. 2.17(2)(h)(v)

Reg. 2.17(2)(h)(vi)

Reg. 2.17(2)(i)

Reg. 2.18(1)(a)(i)

Reg. 2.18(1)(b)

Reg. 2.17(2)(d)

Reg. 2.17(2)(h)(i)

Reg. 2.18(1)(c).

The first nine in the above list are **NOT** covered by the MTES at all. The final three in the above list (Regs. 2.17(2)(d), 2.17(2)(h)(i) and 2.18(1)(c)) are only partially covered by the MTES, so they too will need to be fully addressed by airport operators' TSPs. The reasons are as follows:

- **Reg. 2.17(2)(d)** - Parts 2.7 and 2.8 of the MTES discuss the treatment of 'suspect' passengers, but no provision is made for how this may be done. The same applies to the screening of personal effects, under the same sub-regulation (Parts 2.24-2.28 of the MTES).

- **Reg. 2.17(2)(h)(i)** - The MTES contains information relating to diplomats and other VIPs There is potentially more for operators to include in TSPs than the information found in Parts 2.16 and 2.17 of the MTES.

  Note: For more information about VIPs, see 'Information About VIPs', p. 30

- **Reg. 2.18(1)(c)** relates to procedures to treat unattended and suspect baggage. This is alluded to in Part 6 of the MTES. However, further clarity from airport operators is needed on this issue.

Checked Baggage Screening (CBS)

> *Please note that in relation to CBS, airport operators must ensure that their TSP is not inconsistent with Subdivision 4.1.2 of the Regulations.*

The airports where CBS is required (or in some cases, will be required on and from 1 August 2007) are set out in Reg. 4.29.

If CBS is not required by legislation at your airport, the TSP may state 'N/A – checked baggage screening is not required at this airport under ATSA/ATSR'.

Under Reg. 2.18(1), if CBS is conducted at the airport by the airport operator itself, the TSP must include the measures, equipment and procedures to carry out screening including the:

i. locations where screening is undertaken;

ii. details of the screening equipment used; and

iii. details of the persons operating the screening equipment.

The TSP must also include:

- measures and procedures to ensure that checked baggage is protected against tampering and the introduction of explosives;
- procedures to treat unattended and suspect baggage; and
- measures and procedures to respond to the detection of explosives.

Where the airport operator conducts CBS itself, it does not need to attach its CBS plan to the TSP, provided that it lists substantial measures and procedures in the TSP, and those measures and procedures meet the requirements set out above.

If a screened air service operates from the airport, but the airport operator does not carry out CBS, the TSP must specify the screening authority that does so (Reg. 2.18(2)).

Cargo Facilities with Direct Access to Airside

Under Reg. 2.19, if a screened air service operates from the airport, the TSP must be accompanied by a document listing each facility that has direct access to the airside of the airport, and is responsible for receiving, processing and clearing cargo.

Where the TSP follows the Department's "*Template for writing a Transport Security Program (TSP) - Airport Operators "*, this information can be included in **Appendix E**.

Control of Firearms, Other Weapons and Prohibited Items

> *Please note that in relation to control of firearms, other weapons and prohibited items, airport operators must ensure that their TSP is not inconsistent with Divisions 4.2 and 4.3 of the Regulations.*

For Regulations regarding weapons and prohibited items specifically, refer to Part 4, Divisions 4.2 and 4.3 of the ATSR.

For a list of weapons and prohibited items as defined under the ATSA, refer to ATSA s.9 and Regs. 1.07 and 1.09.

Under Reg. 2.20(1), the TSP must include:

a) measures to deter unauthorised possession of firearms, other weapons and prohibited items; and

b) procedures for dealing with surrendered firearms, other weapons and prohibited items.

The TSP should describe how you will respond to the detection of any firearms, other weapons and prohibited items within your operation.

Under Reg. 2.20(1)(c), the TSP must include procedures for handling and movement of firearms and other weapons.

The airport operator should differentiate between procedures followed by staff, other authorities and passengers within the airport. You should provide details on the procedures that will be used on the ground to ensure the security of firearms and other weapons, including storage.

Under Reg. 2.20(1)(d), the TSP must include procedures for using firearms and other weapons in the airside area or landside security zones. The TSP should also include procedures that apply for using firearms and other weapons in bird hazard control.

Under Reg. 2.20(1)(e), the TSP must include methods for ensuring that staff with a need to know are aware of the restrictions on possessing and using firearms, other weapons and prohibited items within the airport.

Reg. 2.20(2) provides that airport operators must ensure that procedures in the TSP to handle or transport firearms, other weapons and prohibited items are consistent with relevant Commonwealth, State or Territory laws.

Heightened Security Alert

TSPs must address measures for heightened security alerts both:

- When the Australian Government formally raises the Australian national counter-terrorism alert level; and

- When specific threats occur to your operation.

The TSP should demonstrate that the airport operator has allowed for the national counter-terrorism alert level to remain elevated indefinitely. The operator should include measures immediately available, as well as measures for long-term implementation.

Under Reg. 2.21(1), you must set out, in an accompanying document to your TSP, additional security measures and procedures available to reflect your capacity to respond, in the event of a heightened security alert (High or Extreme).

These may include, but do not have to be limited to, increased security guards, increased patrols, 24-hour watches, extra lighting or closing the airport. Where the TSP follows the Department's "*Template for writing a Transport Security Program (TSP) - Airport Operators*", these measures may be shown at **Appendix L**.

Under Reg. 2.21(2)(a), the TSP must set out, in an accompanying document, procedures for responding to and investigating aviation security incidents, including threats and breaches of security.

ATSA s. 99 defines an aviation security incident as:

(a) a threat of unlawful interference with aviation; or

(b) an unlawful interference with aviation.

The procedures should also describe how incidents and breaches will be communicated to and coordinated with relevant authorities.

Unlawful interference with aviation is defined in ATSA s. 10.

Section 10 of ATSA defines 'unlawful interference with aviation' as:

(1) Any of the following done without lawful authority is an ***unlawful interference with aviation*** :

(a) taking control of an aircraft by force, or threat of force, or any other form of intimidation;

(b) destroying an aircraft that is in service;

(c) causing damage to an aircraft that is in service that puts the safety of the aircraft, or any person on board or outside the aircraft, at risk;

(d) doing anything on board an aircraft that is in service that puts the safety of the aircraft, or any person on board or outside the aircraft, at risk;

(e) placing, or causing to be placed, on board an aircraft that is in service anything that puts the safety of the aircraft, or any person on board or outside the aircraft, at risk;

(f) putting the safety of aircraft at risk by interfering with, damaging or destroying air navigation facilities;

(g) putting the safety of an aircraft at risk by communicating false information;

(h) committing an act at an airport, or causing any interference or damage, that puts the safe operation of the airport, or the safety of any person at the airport, at risk.

(2) However, ***unlawful interference with aviation*** does not include lawful advocacy, protest, dissent or industrial action that does not result in, or contribute to, an action of a kind mentioned in paragraphs (1)(a) to (h).

Under Reg. 2.21(2)(b), the TSP must set out, in an accompanying document, procedures for reporting aviation security incidents, or security breaches including occurrences that threaten the security of the airport.

Part 6, Division 4 of the ATSA sets out the requirements for AIPs to report incidents. ATSA s. 104 requires airport operators to report incidents to:

- the Secretary; and
- the Australian Federal Police or the Police Force of a State or Territory; and
- if the incident relates to a part of their airport that is leased or licensed to another person, that other person.

An incident that relates to the airport of another operator must be reported to that other operator. An incident that relates to the aircraft of an aircraft operator must be reported to the aircraft operator (s.104(2) – (3) of ATSA).

Incident reports must follow the format prescribed by the Secretary. If the TSP includes an example, refer to *Notice About How Incident Reports are to be Made*.

Under Reg. 2.21(2)(c), the TSP must set out, in an accompanying document, procedures for evacuation and emergency management in case of an aviation security incident, security threat or breach of security, including:

- an aircraft hijacking;
- a bomb threat; and
- a failure of critical security equipment.

Current procedures for evacuation and emergency management may be included.

ATSA s. 67 sets out the circumstances in which the Secretary may direct that additional security measures will be taken or complied with. A direction made under this section is a 'special security direction'.

Under Reg. 2.21(2)(d), the TSP must set out procedures for responding to any special security direction given by the Secretary, including procedures to communicate directions within the airport, eg. to passengers and other persons within the boundary of the airport.

If appropriate, these procedures could include, but do not have to be limited to:

- steps taken to ensure that a security direction is implemented as soon as possible after it is given, eg. convening an ASC meeting; and
- procedures for communicating the security direction within the security controlled airport and, where appropriate, externally.

Under Reg. 2.21(2)(e), the TSP must set out, in an accompanying document, procedures for raising the awareness and alertness of staff to security threats and their responsibility to report aviation security incidents and breaches.

These procedures should include, but do not have to be limited to:

- provision of training to staff to ensure security awareness and alertness to security threats; and

- internal procedures for employees to report security incidents to management.

Under Reg. 2.21(2)(f), the TSP must set out, in an accompanying document, the details of any other security contingency procedures and plans related to heightened security alerts.

Security Training

The ATSR set out training and qualification requirements for airport security guards and screening officers at Part 5, Divisions 5.2 and 5.3.

Under Reg. 2.02, the airport operator must appoint an SCO who is an employee of the airport operator, in accordance with the TSP. The responsibilities of an SCO are:

a) to facilitate the development, implementation, review and maintenance of the TSP; and

b) to undertake liaison with other AIPs in relation to aviation security matters.

Under Reg. 2.22(1), the TSP must set out:

a) the criteria for selecting the SCO; and

b) any training that must be given to the SCO.

Under Reg. 2.22(2), the TSP must specify, by reference to their positions, the employees, contractors and other persons (other than the SCO) who have been assigned particular security duties and responsibilities.

Under Reg. 2.22(3), the TSP must also set out:

a) their duties and responsibilities;

b) the knowledge, skills and other requirements for the security-related aspects of their positions; and

c) the training or qualifications that satisfy those requirements.

Under Reg. 2.22(4), the TSP must describe the aviation security training programs that will be given to the staff with a need to know. If relevant, TSPs may include training under the 'Securing Our Regional Skies' capability building program.

This requirement is complementary to that required under Reg. 2.22(3)(c), and is meant to ensure that general and threat-specific training is provided to appropriate personnel.

For example, the airport operator may describe any other security-related training to be provided to appropriate personnel, including contingency plan exercises and

exercises designed to test readiness to respond to an act of unlawful interference with aviation.

Barriers

Under Reg. 2.23(1), only the following airports are required to include details of barriers in their TSP:

- Adelaide Airport;
- Alice Springs Airport;
- Brisbane Airport;
- Cairns Airport;
- Canberra Airport;
- Coolangatta Airport;
- Darwin Airport;
- Hobart Airport;
- Melbourne Airport;
- Perth Airport;
- Sydney Airport.

Under Reg. 2.23(2), the TSPs for these airports must:

a) set out the specifications of a barrier sufficient to deter unauthorised access to the airside of the airport; and

b) require the airport operator to construct and maintain a barrier to the specifications set out in their TSP.

INFORMATION ABOUT VIPs

Introduction

Importance of this issue

Proper treatment of all VIPs when undergoing security screening is a critical issue for OTS. Previous incidents have shown that not only can these incidents have immediate aviation security concerns; a mishandled incident can affect Australia's broader bilateral relationships at a whole-of-Government level.

What is a VIP?

There is no one definition of what constitutes a VIP. Different categories of VIPs are entitled to different treatment, and they will all have different expectations of the security screening process. According to the ATSA, VIPs can include the Queen of Australia, the Royal Family, Heads of State, Heads of Government, other Guests of Government and their aides and entourage. Diplomats are also entitled to certain VIP-type privileges.

Policy Position

The Government's position is that all persons travelling on a screened air service must be screened and cleared. The ATSR provide one automatic exemption for the Queen of Australia.

The Act also provides the Secretary the capacity to exempt people from screening on a one-off basis[3]. However, the circumstances would have to be exceptional since exemptions only undermine the robustness of Australia's security arrangements. Accordingly, the Australian Government strongly encourages all VIPs to undergo normal security screening processes at Australian airports.

Screening Processes and Strategies

Standard Screening Process

The screening of passengers and carry-on baggage is a process designed to detect weapons and prohibited items, and prevent their entry into the sterile area and the screened air service.

Passenger and carry-on baggage screening consists of three stages – Primary and Secondary Screening and Explosive Trace Detection.

Screening and clearing is legislated by the ATSA and ATSR. The procedures are detailed in the notice specifying the MTES**.**

Screening Obligations and Requirements Generally

Everybody has the right to be screened in a courteous and professional manner. Particular obligations placed on the screening process include:

- A screening officer must not use more force, or subject a person to greater indignity, than is necessary and reasonable.
- A person must not be screened unless they consent to being screened.
- A screening officer must not force a person to remove items of clothing.
- Where secondary screening techniques are required, a person has the right to request that this be carried out in a private room by a screening officer of the same sex.

Particular Screening Issues for VIPs

Screening of VIPs presents a number of unique challenges:

- Known/unknown departures
    - Not all VIP departures will be known in advance, and not all VIPs will be accompanied by CERHOS officers or other minders.
    - Not all requests for VIP treatment will be able to be verified on the spot.
- Entourage/Minders
    - Previous incidents have shown that while the actual VIP is prepared to undergo screening with a minimum of fuss, members of their entourage can create a situation by demanding particular treatment, and inflaming the situation.
- Inflammatory comments by Screeners
    - There have been reports of occasions where screeners have made comments along the lines of ‘I don’t care who you are’ to VIPs and Diplomats who have questioned the normal security screening process.
    - While it is difficult to assess the validity of claims on the spot, a professional reiteration of the need for screening would generally defuse the situation.
- What is Dignity?
    - Dignity is not defined. What may represent an indignity to one person may be no problem at all to another.

- Cultural issues
    - Different cultural sensitivities will impact the type of treatment expected by particular VIPs.
    - Other countries treat particular VIPs differently and may offer automatic exemptions for a wider group than Australia does.
- Diplomatic Immunity Implications
    - Certain parts of the screening process may be seen as problematic by persons with diplomatic immunity privileges.
    - Request to remove simple items of clothing, such as shoes or belts in public may impinge on dignity.
    - Frisk searches carried out in public areas may also impinge on dignity.
    - Inspection of carry-on baggage may also be seen as intrusive.
    - In the event of such a person entering the sterile area without being cleared there may be restrictions on the ability to restrain and detain them.
- ETD Issues
    - The random and continuous nature of the ETD process sometimes presents particular challenges to the VIP screening process.
    - Some VIPs (and people generally) may feel they have been targeted or treated unfairly if selected for ETD. This has been the cause of previous complaints and confrontations.
    - It is often exacerbated by the fact that the VIP's entourage will stand back and let them pass through screening first. As such, the VIP is often a prime candidate for ETD selection.
    - ETD is an integral part of the screening process, and individual exemptions can not be granted.

Strategies for smooth VIP facilitation

Planning ahead – being of aware of movements where possible:

- Ensuring that the appropriate people know.
- Sensitivity of the bigger picture:
- Being aware that this is an issue that can have large implications.

Awareness of VIP identity and privileges:

- Knowing what categories of people are eligible for particular privileges.

Prior arrangements:

- Agreeing to prior screening arrangements with CERHOS/Department of Foreign Affairs & Trade where possible.

Professional and courteous screener conduct:

- This should happen generally – but especially in response to a request for 'VIP treatment'.

Flexibility in Screening:

- For example, use of private rooms, or involving the screening supervisor.

Keeping a calm head:

- Responding properly and professionally.

Getting the right people to respond:

- Knowing who to call if things go 'pear-shaped'.