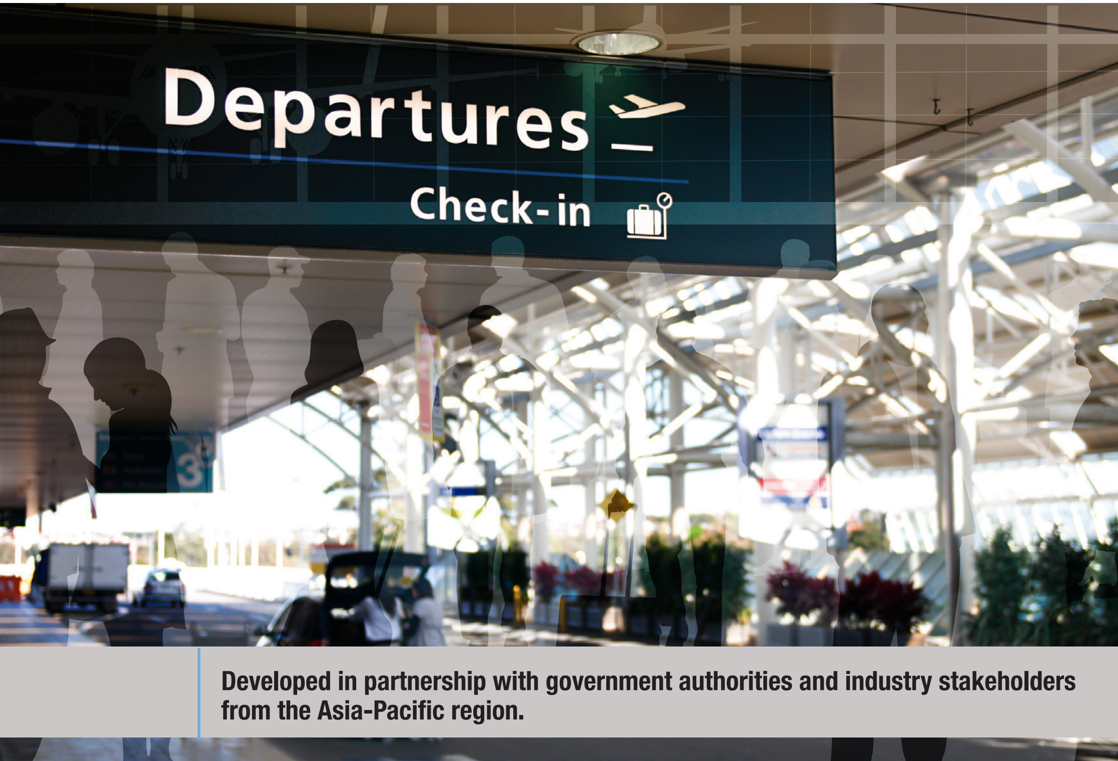
Australian Government

A guide to developing and implementing a Suspicious Activity Identification Program at airports



Developed in partnership with government authorities and industry stakeholders from the Asia-Pacific region.

A guide to developing and implementing a Suspicious Activity Identification Program at airports

Contents

Foreword

Safe and secure transport networks are critical to economic development and promoting trade. Transport security is essential to improving regional infrastructure, and is a vital enabler of trade and industry.

Poor security awareness culture and understanding – together with basic systems for identifying and responding to suspicious activity and behaviour – can expose airports to security risks and threats where there may not be the capacity to prevent or respond to these.

Security awareness at airports needs to increase and guidance is needed to develop and implement Suspicious Activity Identification Programs to manage potential threats.

States that are signatories to the 1944 Convention on International Civil Aviation (also known as the Chicago Convention), which established the International Civil Aviation Organisation (ICAO), are expected to demonstrate compliance with the Standards and (where possible) the Recommended Practices set out in the 19 Annexes to the Convention. Annexes to the Convention have been developed covering, among other things, safety, security, air navigation and facilitation.

Annex 17 – *Security* to the Chicago Convention relates directly to the security of international civil aviation operations.

Recommendation 4.4.5 states:

> *Each Contracting State should ensure that practices are established at airports and on board aircraft to assist in the identification and resolution of suspicious activity that may pose a threat to civil aviation.*

While **Recommendation 3.1.10** states:

> *Each Contracting State should ensure that personnel of all entities involved with or responsible for the implementation of various aspects of the national civil aviation security programme and those authorized to have unescorted access to airside areas receive periodic security awareness training.*

In addition to Annex 17 – *Security,* Document 8973, the Aviation Security Manual provides guidance on achieving compliance with Annex 17. Document 8973 highlights the importance of a robust security awareness regime and a positive security culture as cornerstones of effective aviation security outcomes.

Scope

This handbook provides guidance and tools to help develop, implement and maintain a Suspicious Activity Identification Program.

Each program will be different, as each will be based on the local threat and risk environment.

It is not possible to identify all potential factors within this handbook. In developing a Suspicious Activity Identification Program, industry participants must determine which stakeholders to include, how big or small to make their program, and how their program will operate.

FOR FURTHER INFORMATION SEE THE *SUSPICIOUS ACTIVITY IDENTIFICATION PROGRAM CHECKLIST* AT ANNEX A

There is no reason to believe that all suspicious activity is automatically related to a threat of terrorism or is linked to criminal activity. However, the purpose of a Suspicious Activity Identification Program is simply to **resolve** suspicious acts.

Acknowledgements

This handbook provides guidance on developing and implementing a Suspicious Activity Identification Program that is tailored to the local risk context. Content draws upon extensive operational knowledge and best practice models captured through the Maritime and Aviation Security Awareness Workshops (MASAW) project.

Contributors to this handbook – and participants in the MASAW project – include a range of agencies from Australia, China, Hong Kong Special Administrative Region, Indonesia, Malaysia, New Zealand, Papua New Guinea, the Philippines, Singapore, Timor-Leste, the United States and Viet Nam.

MASAW was managed and funded by the Australian Government as part of its contribution towards meeting APEC transportation priorities. The Department of Infrastructure and Regional Development conducted MASAW to bring regional counterparts and transport industry representatives together to develop this resource for the benefit of APEC economies.

Thank you to all who contributed and, in particular, the Indonesian, Thai and Vietnamese governments for hosting the regional workshops that supported development of this resource.

AUSTRALIA

Australian Government

Department of Infrastructure and Regional Development

AUSTRALIAN FEDERAL POLICE

AFP

AUSTRALIAN FEDERAL POLICE

jetstar.com Jetstar

MELBOURNE AIRPORT

ACI

ASIA-PACIFIC

AIRPORTS COUNCIL INTERNATIONAL

中国民航

CAAC

香港國際機場 HONG KONG INTERNATIONAL AIRPORT

AVSECO

HONG KONG

In cooperation with

ICAO • OACI • ИКАО

ICAO

MINISTRY OF TRANSPORTATION

Angkasa Pura | AIRPORTS

Garuda Indonesia

The Airline Of Indonesia

Incheon Airport

DCA MALAYSIA

MALAYSIA AIRPORTS

CAA

CIVIL AVIATION AUTHORITY OF NEW ZEALAND

Te Mana Rererangi Tūmatanui o Aotearoa

Papua New Guinea

CIVIL AVIATION SAFETY AUTHORITY

PAPUA NEW GUINEA

OFFICE FOR TRANSPORTATION SECURITY

DOTC

MINISTRY OF TRANSPORT

CONNECTING SINGAPORE

CAAS

Civil Aviation Authority of Singapore

CHANGI

airport singapore

Republika Demokratika Timor Lorosa'e

UNIDADE ACÇÃO PROGRESSO

RDTL

Civil Aviation Authority of Thailand (Thai DCA)

AOT

บริษัท ท่าอากาศยานไทย จำกัด (มหาชน)

Airports of Thailand Public Company Limited

U.S. DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

CAAV

Definitions

What is suspicious activity?

> *The actions of an individual or group that is outside the normal acceptable standards for those people or that particular area.*

Suspicious activity may include, but is not limited to:

- putting down a bag or item and then walking away from it
- taking photographs of infrastructure or filming security measures or procedures
- not wearing an ID card in an area where one is required
- unauthorised cargo shipments
- acting nervously, agitated or scared
- repeatedly being at a location, for no apparent reason
- asking unusual or unnecessary questions
- avoiding security personnel or systems.

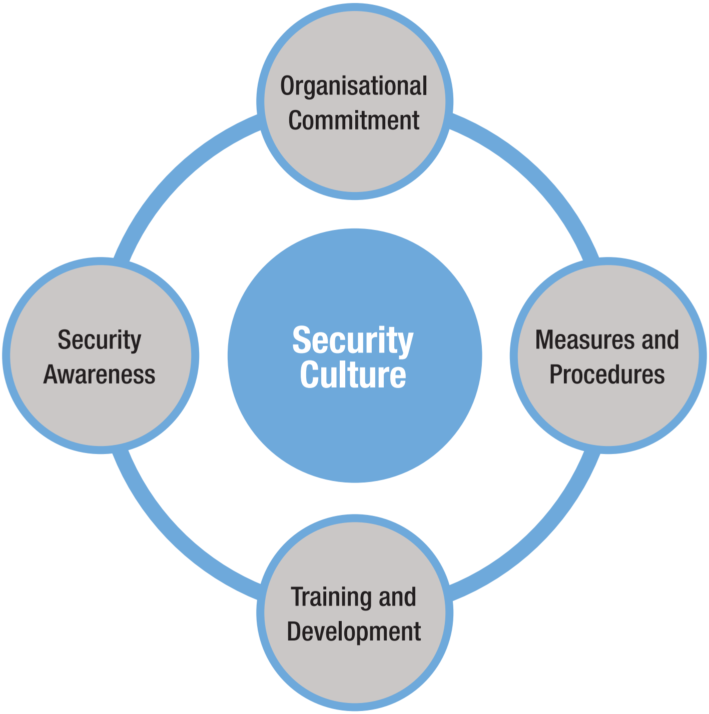
What makes a person suspicious is not their skin colour, gender, ethnicity or position in society. It's what they are doing, where they are or how they are behaving.

What is a Suspicious Activity Identification Program?

A structured process that creates an environment where individuals – through commitment, training and awareness – are encouraged to identify and report suspicious activity, and where reports receive a timely and appropriate response.

What is security culture?

An organisational belief system that permeates all levels of an entity or company's management and staff, and which promotes awareness and individual responsibility for achieving security outcomes.



1. Introduction

Air, sea and land transport operations are essential services that support social and economic development by creating opportunities for travel, trade and tourism.

Recent history has shown there is a genuine threat to the transport sector from terrorist organisations seeking to disrupt operations for:

- significant economic and psychological impact
- vivid media imagery
- mass casualties.

> Even an unsuccessful terrorist attack has the potential to interrupt business continuity and damage customer confidence.

At the same time, criminal elements seek to exploit weaknesses in security regimes to maintain their criminal operations, whether these are small-scale thefts or large-scale transnational organised crime, such as:

- drug importation
- people smuggling
- money laundering
- cyber security breaches.

United Nations Security Council Resolution 2178 (2014) recognises that foreign terrorist fighters in recent years have made extensive use of the transport sector, and calls upon States to help build their capacity to address the threat posed by foreign terrorist fighters. This includes preventing and interdicting foreign terrorist fighter travel across land and maritime borders.

Protecting the transport sector from disruption or exploitation requires a security regime to be established and maintained that is locally specific and based on known threats and risks.

The success or failure of a security regime can in part be attributed to the existence of a healthy and robust ***security culture*** which promotes and rewards high levels of security awareness. A security culture takes time and commitment to develop and mature, but when realised provides an additional, comprehensive and cost-effective layer to the protection of organisational assets.

> Wherever possible, security operations should always seek to utilise existing; infrastructure, technology and (most importantly) people.

There have been a number of developments to improve technology and to help mitigate known threats. However the application of screening/scanning equipment, surveillance systems and access control measures is both expensive and simply not enough on its own. Well-developed and fully-implemented security awareness programs are a way to engage people in the frontline of identifying suspicious behaviour and – more importantly – it is a function they can fulfil while undertaking their normal activities.

> Potentially, the most under-utilised resource available to security managers is the eyes and ears of employees and visitors to their facilities.

2. Concept

In developing a suitable program, consider existing legislation and national policy documents, including for example, **but not limited to:**

- Aviation (Security) Act and Regulations
- Criminal laws
- National Civil Aviation Security Programme
- National Civil Aviation Security Quality Control Programme
- National Civil Aviation Security Training Programme
- Transport Security Plan(s) / Airport Security Plan(s)
- Airline operator security plan(s)
- privacy laws
- data retention/archive laws.

A Suspicious Activity Identification Program is only one piece of the security puzzle, at the centre of which should be a security culture. A security culture is not something that can be instantly implemented—it is something that develops over time through a combination of:

- high-level commitment from management and staff to achieve aviation security outcomes
- appropriately developed and implemented risk-based security measures and procedures
- targeted and recurrent training
- high levels of security awareness among staff.

2.1. Commitment

Establishing a security regime and developing a security culture requires ongoing commitment. It is imperative that senior management demonstrates that it values the benefits of security as a cornerstone of a high performing organisation. It is unreasonable and unrealistic to expect all levels of an organisation to fully participate if there is a lack of senior leadership on the issue.

Commitment is also a long-term requirement. For a security regime to evolve into a security culture, it is vital to maintain communication and education to ensure that motivation is maximised.

> A security culture is when security is viewed throughout all levels of the organisation as a core function and a shared responsibility.

2.2. Training

Effective implementation of security measures and procedures relies on developing and implementing appropriate training modules. As well as legislated training requirements for personnel with specific security roles, it is important to identify additional training that is specific to the operational environment for staff with both security and non-security functions.

A training matrix may help identify all relevant airport workers and visitors, and the appropriate training program for them. In some cases, this may simply be a requirement for security awareness training. In others, it may identify valuable opportunities for staff development.

FOR FURTHER INFORMATION SEE THE *TRAINING MATRIX* AT ANNEX B

2.3. Security awareness

Security awareness is the most basic level of any security training program. All employees should undertake security awareness training to ensure they fully understand their operating environment and how security requirements interact with their daily functions. This basic knowledge allows staff to determine what normal or regular behaviour looks like, and to identify anything irregular.

Security awareness training doesn't need an extensive commitment of time, but it must be regularly revisited to ensure the message and level of understanding is current and consistent. Security awareness can also be communicated to airport visitors through appropriate use of signs, display boards and announcements, and terms and conditions of entry.

2.4. Suspicious activity

A Suspicious Activity Identification Program is in many ways an element of security awareness training. A key objective is to focus stakeholders, staff and visitors on identifying unusual behaviour, and to support this with an effective reporting and response mechanism.

A Suspicious Activity Identification Program involves more than an understanding of the local operational environment. It requires individuals to be proactive and to adopt a level of controlled curiosity or suspicion in the way they observe their work environment. It also requires them to have the knowledge and motivation to react appropriately by bringing their concerns to the attention of the appropriate agency.

3. Developing a Suspicious Activity Identification Program

There are many elements to a successful Suspicious Activity Identification Program that need to be included in the development stage.

3.1. Threat environment

Threat is determined by assessing the **INTENT** to commit an act and the **CAPABILITY** to carry it out successfully. Both intent and capability have to exist for the threat to be considered genuine.

THREAT = **INTENT** X **CAPABILITY**

For example, if a man says he is going to kill another man, it could be said that the intention is real. However, if a river separates the two men and no weapon is involved, then the capability to carry out the intention doesn’t exist, and so the threat is not real or genuine.

A realistic and rational understanding of the local threat environment is a basic premise for developing any security regime. It is this understanding of the threat that allows risk assessment methodology to be applied and the appropriate mitigation strategies to be identified.

Airports provide unique environments and specific threats, however recent history shows that the popularity of civil aviation operations as a target has created new and innovative ways to breach security and exploit vulnerabilities. That said, there are a number of known threats that must always be considered, including:

- person-borne improvised explosive devices (PBIED)
- vehicle-borne improvised explosive devices (VBIED)
- lone wolf attacks
- insider threats
- cyber attacks
- organised crime.

In all of these threat scenarios, it is highly likely (and to be expected) that a degree of reconnaissance will occur before an attack. In such circumstances, high profile security awareness, a Suspicious Activity Identification Program, and the efforts of proactive staff may provide sufficient evidence of a robust security regime to detect or deter any threats before they can be implemented.

3.2. Risk assessment

Generally, risk is considered to be the **LIKELIHOOD** of an event occurring and the **CONSEQUENCE** if it does. In a security environment however, likelihood becomes difficult to determine and so it must be considered in the context of existing threats and known vulnerabilities.

RISK = LIKELIHOOD X CONSEQUENCE

Where…

LIKELIHOOD = THREAT X VULNERABILITY

Assessing security risk therefore is like an equation that requires an understanding of the threats to operations, identified vulnerabilities (or gaps) in your security regime and an assessment of the consequences if those vulnerabilities are exploited.

By implementing a robust risk assessment methodology, an entity can establish a level of risk tolerance relative to the local threat and risk context. This also ensures the mitigation strategies identified and implemented are justifiable, well considered and likely to be effective.

Annex 17– *Security* to the Chicago Convention details a number of Standards and Recommended Practices for regulators and operators within the civil aviation system. These include how to undertake a risk assessment as part of the development of security measures and procedures.

3.3. Risk context

Establishing the risk context for an operational environment enables measures and procedures to be identified and implemented that mitigate threats with an unacceptable level of risk. While it is not possible to mitigate all risk, adopting a risk assessment methodology and developing an understanding of the risk context allows for a considered and targeted approach.

Managing risk is an ongoing process for any organisation. Any change to an operational environment or infrastructure can have an impact (positive or negative) on the mitigation strategies that have been implemented. It is essential that senior executive and appropriately qualified staff regularly reassess the risk context.

FOR FURTHER INFORMATION SEE *THREAT AND RISK* AT ANNEX C

3.4. Legislation and policies

An important consideration in developing a Suspicious Activity Identification Program is the impact of existing legislation and policies, and avoiding any conflicting requirements. It is important to review legal and policy documents to identify roles and responsibilities that may currently be assigned to specific agencies or organisations.

Implementation will also be more effective if a whole-of-airport scheme can be designed in a way that is complementary of any individual organisation’s procedures. This also highlights the importance of stakeholder engagement in the development stage of any Suspicious Activity Identification Program.

3.5. Stakeholder engagement

To be successful, a Suspicious Activity Identification Program must identify all relevant stakeholders. This may require different levels or tiers of engagement to allow for high level participation by stakeholders that are key to the program's development, and lower level engagement for those that will be recipients of the end product.

It is through wide-ranging and inclusive consultation that all relevant considerations can be included and a level of commitment can be developed. Individuals are more likely to willingly participate if they have contributed during the development process.

3.6. Government – industry partnership

Depending on the local circumstances, it is highly likely that a Suspicious Activity Identification Program will require enhanced cooperation between government agencies and (potentially privately owned) aviation industry participants. The degree to which this relationship can be viewed as a partnership will enhance the outcomes.

It is also essential that a lead agency is identified to champion the program. Depending on the local operating environment, this may be a regulatory authority, a response agency or the operator. Whatever shape the program takes, there is a strong need for coordination, cooperation and collaboration.

3.7. Resources and structures

Developing, implementing and maintaining a Suspicious Activity Identification Program requires dedicated and specific physical, financial and intellectual resources. These include:

- ongoing senior management commitment across a range of stakeholders
- funding for training, communication strategies, IT requirements and office services
- staff to receive reports and implement response procedures.

Clearly defined responsibilities for resourcing must be determined. Stakeholders to be included in this process include airport operators, law enforcement agencies, intelligence agencies, border agencies and security service providers.

Consider using existing structures and forums to support the Suspicious Activity Identification Program such as the Airport Security Committee, emergency response program/airport contingency plan, and emergency response committee.

3.8. Information management

Specific consideration needs to be given to:

- how and what reported information is captured
- how it will be used
- how and who it will be shared with
- feedback mechanisms.

A back-of-house system that doesn't enable data retention and analysis will serve little purpose beyond being a clearing-house for reported events. At the same time, the right information in the right hands can be useful in determining whether there are patterns in the types and locations of events. Establishing a database to enable trend and causal analysis could provide useful information and help to identify areas where improvements can be made.

4. Suspicious Activity Identification Program implementation

A Suspicious Activity Identification Program is a baseline security counter-measure that should complement a broader regime of risk-based preventative security measures and procedures. It should include numerous elements that are mutually important, including:

- organisational commitment
- heightened awareness
- educating people about what to look for
- creating a mechanism for reporting
- developing processes for responding to reports
- ongoing engagement to maintain focus
- regular internal review.

4.1. Benefits

There are a number of significant benefits associated with the successful implementation of a well-developed Suspicious Activity Identification Program. It:

- is a relatively low-cost preventative security measure to introduce
- can have little or no ongoing costs
- doesn’t require an in-depth initial training component
- provides an enhanced overall level of security awareness
- uses existing staff in their normal operational environment and without unnecessarily increasing their responsibilities

- promotes a sense of communal responsibility for security
- contributes to the development of a security culture
- provides positive reinforcement for the proactive responses of staff
- creates a mechanism for capturing information and intelligence
- enables a timely response to reports
- supports the resolution of reported events
- is an opportunity to benefit from the observations of visitors to the airport
- is a well-publicised deterrent to potential attackers.

4.2. Communication

A communication strategy will be a determining factor in whether the Suspicious Activity Identification Program succeeds or fails. Identifying the correct audience, developing key messages, delivering clear information that is easily understood, and regularly revisiting core messages are all important elements.

Communication must be targeted to ensure stakeholders remain focused on the objectives. This may require different tactics and channels to ensure that senior executive staff as well as front line operators and the travelling public can be engaged and mobilised. Communication channels could include official directives, newsletters, magazines, e-tickets, flight information boards and advertising.

To ensure high-level commitment is maintained for the program, regular updates must be provided to key stakeholders, whether this is through the board of airline representatives or Airport Security Committee meetings. Updates should include details of any trends in reporting and what efforts have been undertaken to maintain engagement with the program.

4.3. Training

The level of training required by individuals will vary depending on their roles and responsibilities. Those with responsibility for responding to reports of suspicious activity will need to have an in-depth understanding of the operating environment and emergency response procedures.

4.4. Reporting

Appropriate reporting mechanisms need to be established and details of how reports are made need to be clearly understood by all program participants. Reporting should be as simple as possible and made available to all stakeholders, irrespective of what part of the airport environment they work in.

It is also important that reporting information is captured in a format that allows ongoing research and analysis.

An individual report that had no significant outcome at the time of its distribution may prove to be crucial to thwarting a potential future event when considered in relation to a number of associated reports. The level of detail that is recorded and the mechanism for capturing information are essential considerations.

FOR FURTHER INFORMATION SEE AN EXAMPLE OF A *REPORTING TEMPLATE* AT ANNEX D

4.5. No blame

A key element in any safety or security management system is the importance of a ‘no blame’ culture. This requires systems that support individuals making reports, even in situations where they need to admit to making a mistake.

Fear of blame or punishment will more often than not result in a wall of silence and lack of action. Individuals need to understand that a mature organisational security culture can accept that humans make mistakes without imposing immediate punitive measures.

4.6. Response

The response mechanism needs to be appropriately reactionary to ensure staff and visitors to the airport continue to make reports. This will require coordination with the law enforcement and security agencies that will provide the initial response within the airport environment.

A suite of standard operating procedures should be developed to deal with a range of likely scenarios. These procedures must be regularly tested for effectiveness and can be included as a component of any airport security exercise.

Consideration may also be given to the Airport Emergency/Contingency Plan when developing the response mechanism for the Suspicious Activity Identification Program.

4.7. Command and control

Clear lines of command and control must be established and clearly articulated for normal operations. Additional contingencies should be developed in the event of a heightened threat situation or change in the risk context.

While it may be appropriate for staff and security personnel to assess suspicious acts/items during normal operations, it may be prudent to use law enforcement or suitably qualified specialists in times of higher threat. Roles and responsibilities need to be clearly stated and completely understood.

4.8. Increased threat environment

It is important to develop strategies for a general increase in the overall threat environment. This may include adjustments to the tone and frequency of messaging that is relayed to staff and visitors to the airport.

Well-developed (and tested) additional measures will support ongoing facilitation of passengers (where applicable) and normal operations. The aim is to increase awareness, not to promote fear and panic.

4.9. Quality control

A review of engagement with the Suspicious Activity Identification Program should be incorporated into normal quality control activities. This may even take the form of a ‘test’ to see if staff remains proactive and conscious of suspicious acts/items.

Incorporating quality control outcomes into broader considerations of the threat environment and risk context will also support a more holistic approach to the overall security regime. Security audits, inspections, tests and surveys will help identify weaknesses or vulnerabilities in existing security measures and procedures.

FOR FURTHER INFORMATION SEE THE *AUDIT CHECKLIST* AT ANNEX E

4.10. Feedback

An important component to the success of the Suspicious Activity Identification Program is feedback to those individuals who make reports. People's enthusiasm for engaging with the program (and remaining engaged) will be directly impacted by the ease of reporting, the timeliness of the response and the effort to contact the reporter after the event to advise them of the outcome.

Consideration could be given to introducing a reward and recognition component which could encourage employees to embrace the importance of and actively participate in the program. Types of reward and recognition benefits could include monetary reward, certificates of appreciation, special mentions in organisational newsletters or positive media exposure.

4.11. Theme

A theme, motto or tag line could be considered to help reinforce the program's intent and inspire action. The selected theme would need to make it clear to people what they need to do if they observe suspicious behaviour or identify a suspicious occurrence.

Examples include:

- **See It, Hear It, Report It** (Airport Watch, Australia)
- **If You See Something, Say Something™** (Department of Homeland Security, USA)

5. Case Studies

The following case studies demonstrate successful suspicious activity identification programs.

5.1. Airport Watch

The Airport Watch program was developed by the former Department of Infrastructure and Transport's Office of Transport Security in partnership with the Australian Federal Police (AFP). It is based on the well-known community program 'Neighbourhood Watch' and allows people working at, or travelling through airports, to more easily report suspicious activity to the AFP.

The AFP operates at Australia's international airports and provides a first-response capability to potential terrorist attacks, an immediate policing response to crime and disorder incidents, and investigates serious and organised crime.

Airport Watch complements the AFP's existing capabilities, which include community policing, a counter-terrorist first response capability, air security officers, joint intelligence teams, joint investigation teams, bomb appraisal officers, and firearms and explosive detection canines.

The Airport Watch call to action is **"See it, Hear it, Report it"**.

If members of the transport community see something unusual, notice any suspicious behaviour or hear a threatening or unusual conversation, they can contact the AFP.

The Airport Watch model is a low cost preventive security measure. It seeks to complement existing physical and technology-based measures and to enhance security in publicly accessible areas at our major airports.

http://www.afp.gov.au/policing/aviation/airport-watch

5.2. America’s Water Way Watch

Developed by the United States Coast Guard, this national public outreach program encourages people living or working on or near the water to report suspicious activity to the US Coast Guard or the responsible authorities.

The following is an excerpt from this successful initiative.

> This nationwide initiative is similar to America’s Neighbourhood Watch program. It builds on many local and regional programs and urges citizens who spend time near or on the water to adopt a heightened sense of awareness towards unusual events or individuals they may encounter in or around ports, docks, marina, riversides, beaches, or waterfront communities.
>
> Citizens are provided with guidance (accessible online and downloadable posters, wallet cards etc.) on what is meant by suspicious activities and where to look for these. America’s Water Ways program uses the SETS system for identifying suspicious activity.

Identifying suspicious activity

YOU encounter numerous people and situations while working, living or recreating in our nations ports and waterways. During these encounters you could see something that might indicate a terrorist activity is being planned. Knowing how to recognise and respond to terrorism warning signs could enable you to prevent the next act of terrorism. The acronym **SETS** will help you understand the basic steps and indicators.

SETS	
S	**Surveillance** *Surveillance involves photography, videotaping, drawing and/or mapping, or other means of monitoring a potential target.*
E	**Elicitation** *Elicitation involves asking detailed questions in an attempt to gain knowledge of hidden or proprietary information.*
T	**Tests of security** *A test of security is a tool used to develop timelines of authoritative response to a particular incident or occurrence. Staging an incident can be done to determine access vulnerability and/or establish a timeline for later use.*
S	**Suspicious behaviour** *Suspicious behaviour is displayed behaviour that is out of place or out of character with the environment. Remember people are not suspicious. Behaviour is!*

Citizens are also provided with guidance on how make a proper description of a person, boat or vehicle using the CYMBALS method.

CYMBALS

Never use race or religion as an indicator of suspicious activity. Always rely on the idea that what you are observing is like a puzzle. If your instincts suspect suspicious activity, and you have observed a person's/group's actions that you can report to back up your instincts and feelings, then you can report your observations using the CYMBALS method described below.

	People	Boats	Vehicles
C	Color (hair, eyes, skin)	Color (paint, markings, etc)	Color (paint, markings, etc)
Y	Year (of birth, approximate age)	Year (of manufacture, approximate age)	Year (of manufacture, approximate age)
M	Make (race, ethnicity)	Make (make and model of boat)	Make (make and model of vehicle)
B	Body (height, weight, build, etc)	Body (length, type: cruiser, runabout, PWC, etc)	Body (sedan, truck, SUV, 4/2 door, etc)
A	Attire (clothing, description, dress, etc)	Accessories (name, antennas, flag, inboard/outboard)	Anything else (dents, stickers, rims, etc)
L	Looks (hair, scars, tattoos, facial hair, etc)	License/ registration number	License plate number
S	Sex (male, female)	State of registration	State of registration

Citizens are to report suspicious activities using the CYMBALS method above to America's National Response Centre at 877-24WATCH in the first instance unless there is an immediate danger to life or property.
http://americaswaterwaywatch.uscg.mil/home.html

Annexes

These supporting tools were developed to provide you with further information to assist with the development and implementation of your Suspicious Activity Identification Program. Please note that these supporting tools were designed as high level guidance materials and will not be relevant in all situations. You may want to amend or develop additional supporting tools tailored to your situation.

ANNEX A: Suspicious Activity Identification Program checklist

The following checklist is designed to highlight considerations in developing and implementing a Suspicious Activity Identification Program.

Concept

- □ Clarify current threat environment (security and criminality).
- □ Source current risk assessment to identify key areas and assets to protect.
- □ Identify legislative/governmental policy requirements.
- □ Refer to existing security program and SOPs.
- □ Develop business case for development and implementation of SAP.
- □ Develop business case for executive consideration.
- □ Obtain executive commitment to the program.

Development

- □ Identify key stakeholders in the development of the program.
- □ Identify participants in the roll out of the program.
- □ Conduct initial meeting to discuss with stakeholders and obtain commitment.

Resourcing

- □ Identify resources required based on scale and scope of agreed SAP.
- □ Obtain resources (financial, personnel, operational space etc).

Content

- □ Develop SOPs, including checklists, reporting forms and documentation.

Training

- □ Develop SAP training program.
- □ Develop guidance material for staff.
- □ Undertake training for staff with distinct roles and responsibilities.

Communications

- □ Develop a communication strategy.
- □ Develop promotional posters/signage to be used.

Reporting and response

- □ Establish a reporting and response mechanism.
- □ Ensure the reporting and response mechanism is operating effectively.
- □ Develop recording mechanism for capturing details of incidents and events.
- □ Develop internal/executive reporting mechanism for outcomes of program.

Monitor and review

- □ Undertake analysis of reported information.
- □ Prepare summary reports for executive reporting.

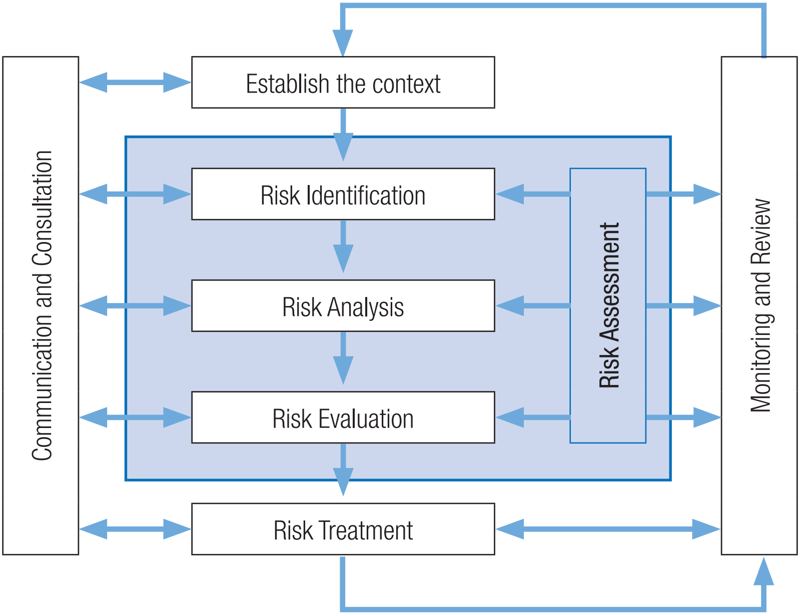
ANNEX B: Training Matrix

The development of a training matrix may assist in identifying key stakeholders and the training needs that are related to their roles. All airport staff and visitors should be required to undergo some form of security awareness training, which may include elements of a Suspicious Activity Identification Program.

	Aviation Security Inspectors	Aviation Security Officers	Aviation Security Guards	Aviation Security Screening Officers	Airport Employees: Primary	Airport Employees: Secondary	Airline Employees: Primary	Airline Employees: Secondary	Air Traffic Service Employees	Cargo Agent Employees	Catering Company Employees	Other Regulatory Authorities	Ad hoc Contractors	Passengers/Airport Visitors
Aviation Security Legislation	✓	✓	✓	✓								✓		
International Obligations	✓	✓	✓	✓								✓		
Security Programs	✓	✓	✓	✓								✓		
Airport Environment	✓	✓	✓	✓	✓		✓		✓	✓	✓	✓	✓	
Historical Threats to Aviation	✓	✓	✓	✓										
Threat Factors	✓	✓	✓	✓										
Weapons and Prohibited Items		✓	✓	✓	✓		✓							
Improvised Explosive Devices		✓	✓	✓										
Screening Passengers and Baggage				✓										
Searching Passengers and Baggage		✓	✓	✓										
Use of X-ray Equipment				✓										
Use of Metal Detection Equipment				✓										
Aircraft Search		✓	✓	✓			✓							
Dealing with Armed Offenders		✓	✓	✓										
Hijack Response Procedures		✓	✓	✓	✓		✓		✓	✓		✓		
Bomb Threat		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Foot and Mobile Patrols		✓	✓	✓										
Access Control Procedures		✓	✓	✓	✓		✓		✓	✓	✓	✓	✓	
Identity Card Verification		✓	✓	✓	✓		✓		✓	✓	✓	✓		
Aerodrome Surface Movements	✓	✓	✓	✓	✓		✓		✓	✓	✓	✓	✓	
Aeronautical Radio-Telephone Use		✓	✓	✓					✓					
Security Awareness	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Suspicious Activity Identification	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Lead Auditor	✓													
Risk Management	✓				✓		✓							

ANNEX C: Threat and risk

Risk management is vital to the process of determining and developing appropriate ways to prevent, or minimise, the impact of a security event. It is through a well-informed understanding of the (threat) context, which allows for risks to be identified, analysed and evaluated. Effective risk assessment supports the treatment/mitigation of risks to protect assets – including people, information and infrastructure – in a measured way.



Basic principles of preventative security involve implementing layered measures and procedures designed to:

- deter
    - *security is clearly good at reducing the likelihood of an attempt to breach it*
- delay
    - *security infrastructure is able to slow them down and increase the chance of detection*
- detect
    - *security measures and procedures ensure breaches are identified in a timely manner*
- defeat
    - *measures are in place to appropriately respond to any incident.*

ANNEX D: Reporting template

This reporting template sets out information you may want to capture and record.

Report Number:		**Name of Officer Receiving Report/ Signature:**			
Date of Incident:		**Date Report Received:**			
Time of Incident:		**Time Report Received:**			
Reporting Agency:		**Reported By:**			
Incident Category/ File under:	***Aviation Related*** Suspicious person/ surveillance of systems Unattended bag Suspicious item Bomb threat	***Regulatory Compliance*** Access control breach	***Criminal*** Theft Other crime Drugs	***Terrorism*** Act of unlawful interference	***Other***
Description of Incident:					
Method of Reporting:	Hotline Email	Report Form	In Person	Other:	
Actions Taken:	Preventative	Corrective			
Actions Taken Description					
Information Disseminated To:		Date/Time Information Disseminated:			
Action Taken by Agency (if any):					
Appropriate confidentiality and protection of information statement, if applicable					

ANNEX E: Audit checklist

Suggested audit questions

Is the information on how to report an incident available to all those who need to know?	Yes	No
Does the reporting provide sufficient information?	Yes	No
Do the reporting categories fully identify incidents?	Yes	No
Do the reporting categories provide sufficient information to undertake a trend analysis?	Yes	No
Are the reports being retained and stored appropriately?	Yes	No
Is the confidentiality of reports being maintained?	Yes	No
Are the reports being resolved?	Yes	No
Are the reports being closed out appropriately?	Yes	No
Is feedback being provided where appropriate?	Yes	No
Is information being disseminated to appropriate stakeholders? Check if more information is required.	Yes	No
If training is required – has it been confirmed that training has been undertaken?	Yes	No
Are the reporting procedures correctly followed by the security personnel on duty?	Yes	No