



For Official Use Only

Airport CCTV – data handling

Procedural Instruction

This instruction provides guidance in relation to correct Closed Circuit Television (CCTV) data handling procedures, including the release of CCTV data information and recorded media to other government agencies.

Approval Date	21 May 2018
Date of Review	21 May 2019
Contact	s. 22(1)(a)(ii) @abf.gov.au
Document ID (PPN)	TI-742
TRIM Reference	OPD2017/203854

Released by Department of Home Affairs
under the Freedom of Information Act 1982

For Official Use Only
OFFICIAL

For Official Use Only

Table of Contents

1. Introduction	4
1.1. Background	4
2. Scope	4
2.1. In Scope	4
2.2. Out of Scope	4
3. Glossary	5
4. Procedural Instruction	6
PART A – CCTV data handling	6
4.1. Privacy	6
4.2. Disclosure of information	6
4.3. Requests from external agencies	6
4.4. CCTV camera sharing with non-government agencies	7
4.5. Evidentiary requirements	7
4.6. Removable storage media	8
4.7. Managing digital video recordings	8
4.8. Copy to DVD or CD	8
4.9. Creating master and working copies	9
4.10. Handling DVDs and CDs	9
PART B – Release of Information to other Government Agencies	10
4.11. Request by external agency	10
4.12. Capture information	10
4.13. Release of media	11
4.14. Record keeping	11
4.15. Compliance and efficiency reporting	11
5. Accountability and responsibilities	12
6. Statement of Expectation	12
7. Related Framework documents	12
7.1. Policy Statement	12
7.2. Procedural Instructions	12
8. References and legislation	13
8.1. Australian Border Force Act 2015	13
8.2. Freedom of Information Act 1982	13
8.3. Crimes Act 1914	13
9. Consultation	13
9.1. Internal consultation	13
9.2. External consultation	13
10. Document details	14
10.1. Document change control	14

Released by Department of Home Affairs
under the Freedom of Information Act 1982

For Official Use Only

10.2. Approval	14
11. Appendices	15
11.1. Attachment A – B1203 – Request for CCTV information (external agency)	15
11.2. Attachment B - Control Room Release of Information Log Book	16
11.3. Attachment C –Sample label template	17

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

For Official Use Only

1. Introduction

1.1. Background

Given the sensitive nature of Closed Circuit Television (CCTV) data, clear guidelines are required for the correct handling and storage of CCTV data, including privacy considerations and the destruction of CCTV data.

Release of CCTV data externally is a sensitive and must only occur in accordance with policy and legislative requirements. Section 44 of the *Australian Border Force Act 2015* (Australian Border Force Act) sets the framework for the release of Australian Border Force (ABF) information to other agencies.

2. Scope

2.1. In Scope

This procedural instruction provides guidance to Australian Border Force (ABF) officers in relation to correct Closed Circuit Television (CCTV) data handling procedures, including the release of CCTV data information and recorded media to other government agencies.

Given the sensitive nature of CCTV data, clear guidelines are required for the correct handling and storage of CCTV data. This includes privacy considerations and the destruction of CCTV data.

This procedural instruction applies to staff in the aviation environment.

2.2. Out of Scope

This procedural instruction does not cover how to operate the CCTV system.

Clearance of travellers and/or goods under the *Customs Act 1901* (Customs Act).

Released by Department of Home Affairs
under the Freedom of Information Act 1982

For Official Use Only

3. Glossary

Table 1 – Common terms and definitions used in this instruction

Term	Acronym (if applicable)	Definition
Air Border Security Control Room	ABS	Is a Closed Circuit Television Control Room that uses techniques and methods to protect travellers, staff and planes that use the airports from accidental/malicious harm, crime and other threats.
Australian Border Force	ABF	The Australian Border Force is an agency within the Home Affairs portfolio responsible for offshore and onshore border control enforcement, investigations, compliance and detention operations in Australia.
Australian Border Force officer	ABF officer	An ABF officer is an Immigration and Border Protection worker (see section 4 Australian Border Force Act) authorised to perform border clearance duties.
Closed Circuit Television	CCTV	Is a system of video monitoring at Australia's international airports and seaports.
Closed Circuit Television Operator		A CCTV operator works in a central control room, monitoring and controlling a bank of screens.
Compact Disc	CD	Is a digital optical disc data storage format.
Digital Video Disc	DVD	Is a digital optical disc storage format. Has a higher storage capacity.
Digital Video Recorder	DVR	Is an electronic device that records video in a digital format to a disk drive, USB flash drive, SD memory card or networked mass storage device.
Super Video Home System	SVHS	Analog video recording on tape cassettes.
Write once read many	WORM	Is a data storage device in which information, once written cannot be modified.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

For Official Use Only

4. Procedural Instruction

PART A – CCTV data handling

4.1. Privacy

Due to the sensitive nature of camera surveillance, management of the national CCTV network must be in accordance with existing legal frameworks and must be maintained with a high standard of integrity and accountability at all times.

The following privacy principles apply:

- Australian Border Force (ABF) officers must treat all information gathered through CCTV as sensitive and make themselves fully conversant with relevant policy regarding the handling and release of any information, recorded or otherwise, obtained through the CCTV system
- recorded images must be collected through lawful means in accordance with the *Privacy Act 1988* (Privacy Act)
- recorded images must be retained for enforcement and regulatory evidentiary purposes or at the request of intelligence agencies. All other recorded images must be overwritten in accordance with system requirements
- CCTV data must only be used by other law enforcement and regulatory agencies for the purposes of investigating whether an offence has been committed against the law of the Commonwealth of Australia or a territory or for the performance of its functions on the understanding that it will not be disclosed or further produced except where required or permitted by law.

4.2. Disclosure of information

Disclosure of information must be in accordance with:

- Section 44 of the *Australian Border Force Act 2015* (Australian Border Force Act)
- *Freedom of information Act 1982* (Freedom of Information Act)
- Section 70 of the *Crimes Act 1914* (Crimes Act).

Under no circumstances should CCTV data be released from any control room or Air Border Security (ABS) room or other place without the appropriate approval and documentary handover as per procedures outlined in Part B of this Procedural Instruction.

4.3. Requests from external agencies

ABF cannot mutually share camera feeds with any other port authority or agency, except where there is a legislative requirement or a formal agreement (e.g. Memorandum of Understanding) in place.

The CCTV system will be available to other appropriate/relevant law enforcement agencies for tasks on a needs and priority basis subject to release of information being in accordance with the provisions of Section 44 of the *Australian Border Force Act 2015*. External stakeholders are required to lodge tasking's requests in the same manner as internal requests.

The ABF officer who is authorised is to complete the *Authority to Disclose Immigration and Border Protection information*. The ABF officer must be satisfied that a training course has been completed. Once complete,

Released by Department of Home Affairs
under the Freedom of Information Act 1982

For Official Use Only

the ABF officer is to hand the *Authority to Disclose Protected Information – General and Request for CCTV Information (external agency)* forms to a CCTV operator for action.

The Authority to Disclose Immigration and Border Protection information form does not need to be completed if an ongoing authorisation is in place, authorising the disclosure to the recipient agency.

4.4. CCTV camera sharing with non-government agencies

The CCTV cameras can also be shared through legal contracts or formal agreements with Airport Owners/Operators based on the following conditions:

- feeds will only be provided from fixed cameras in non-sensitive areas of ABF controlled area at airports
- non-sensitive areas include all areas except the entry and outwards control points and the secondary examination areas
- recording and disclosure of CCTV data to third parties will not be permitted under any circumstances.

To obtain access to cameras owned by airport operator/owner, the following questions need to be answered before requesting access:

- is the camera operationally critical to ABF?
- will a fixed camera be sufficient for our purposes?

Any queries or requests regarding CCTV camera sharing or access should be directed by email s. 22(1)(a)(ii) [@homeaffairs.gov.au](mailto: @homeaffairs.gov.au) to Major Capability, CCTV & Enforcement Communications Branch.

4.5. Evidentiary requirements

When an incident or offence has occurred and there is a requirement to preserve CCTV data for evidentiary purposes, the following steps should be followed:

- identify relevant recorded images on the Digital Video Recorder (DVR)
- ensure that the required data is not recorded over while arrangements to save the data are being made. **S. 47E(d)**

- transfer digital data from the hard drive to a removable medium, such as a DVD or CD, in a format that allows accurate replay and production of the CCTV data. Two copies should be made – one being a master copy and the other a working copy. The master copy is retained for accountability and audit purposes
- if not using an already labelled DVD/CD, label all DVDs/CDs and tapes with the information contained in the sample template at (**Attachment C**). This can be by hand, sticker or other label
- record details in the relevant register
- release of CCTV data must occur in accordance with section 44 of the *Australian Border Force Act 2015* (Australian Border Force Act)
- master copies of CCTV data must be stored in accordance with the provisions of the Department of Home Affairs Security Handbook located on the Intranet.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

For Official Use Only

4.6. Removable storage media

Removable storage media is designed to be removed from a CCTV system. Examples include portable hard disks (including hard disk caddies), DVDs, CDs, floppy disks, tapes, smartcards, flashcards and thumb drives.

All removable computer disks, tapes, floppy disks, tapes, smartcards, flashcards, portable memory devices and digital photographs are to be marked conspicuously to indicate the security classification of the stored data. Current policy states that unless otherwise specified, all portable CCTV storage media must be marked with a PROTECTED security classification. For further information, see *Procedural Instruction: Airport CCTV Data Security Classification*.

Removable storage media must also be marked with the following caution (See *Attachment D* for copy of the template):

- *This disc is made available to the recipient for the performance of the recipient's functions in investigating whether an offence has been committed against a law of the Australian Commonwealth or an Australian State or Territory. This information is disclosed on the understanding that it will not be used or further disclosed except for the purpose for which it was provided by Australian Border Force or otherwise as required or authorised by law.*

Removable storage media containing classified information must be stored in accordance with the Department of Home Affairs Security Handbook requirements for information of that classification. The required class of container is determined by the classification of the information on the media and the physical security standard of the area in which the container is located. The effective classification level of the media may be reduced by the use of appropriate encryption. For further information, see *Procedural Instruction: Airport CCTV Data Security Classification*.

4.7. Managing digital video recordings

The digital CCTV system uses storage devices in the form of hard disk drives for the direct storage of video files. Due to the limited capacity of hard drives, data stored on hard drives is automatically overwritten after a pre-set time. Prior to CCTV data being overwritten, some or all of the recorded images may be transferred to removable storage media on a case-by-case basis.

There are several types of recording medium suitable for use in copying digital video images from fixed hard drives:

- Magnetic tape, including conventional VHS videotape or Super VHS (SVHS) videotape.
- Non-reusable removable medium or WORM (Write Only Read Many) medium including:
 - CD+R
 - DVD+R
- Reusable, removable, non-tape media, memory cards including:
 - Portable Hard Drives
 - CD+R
 - DVD+R.

For reasons of security and data integrity only media such as DVD+R and CD+R should be used for creating copies, unless there is a specific reason to use other forms of recording media and permission from the relevant Supervisor and or Manager has been received.

4.8. Copy to DVD or CD

In order to preserve CCTV data indefinitely it must be copied on to portable recording media, generally DVD+R or CD+R. Once the data has been successfully copied onto DVD+R or CD+R the original data on

For Official Use Only

the local drive of the computing system should be deleted. Where CCTV data is used for evidentiary purposes, two copies should be made. For routine inquiries or review purposes, only one copy may be required.

The first copy is to be identified as the master copy and will be labelled and treated as such. A working copy is usually produced simultaneously, or immediately after the master is produced. The working copy is the version that will be used as part of an investigation and to assist in the preparation of the prosecution file.

Transfer to DVD or CD should be carried out as soon as possible to reduce the time and opportunity for alteration to original images stored on the hard drive. For evidentiary purposes 'bit for bit' copies such as master and working copies are regarded as the same as original CCTV data stored on a hard drive. This does not remove the necessity to protect the master as an exhibit.

s. 47E(d)

4.9. Creating master and working copies

The Master copy should be:

- on Write Once Read Many (WORM) removable media
- labelled as MASTER Copy, including date and time of recording and camera details (as per the template provided in Attachment D)
- stored in a form and manner, with software if required, so that the images may be viewed in the future
- placed in a suitable protective case, sealed and retained in secure storage in accordance with exhibit protocols
- copied in the same format as it was first captured on original hard drive.

The master copy should not be used, except to produce additional working copies when no working copies are available to copy, or by order of the court to establish authenticity.

The Working copies should be:

- on WORM removable media
- where possible, made at the same time as the master copy, either directly from the hard drive or made at a later time from the master copy
- labelled as WORKING Copy and include date and time of recording and camera details
- stored in a form and manner, with software if required, so that the images may be viewed in the future
- copied in the same format as it was first captured on original hard drive.

4.10. Handling DVDs and CDs

Digital media should be stored in clean environments, avoiding strong light and chemical contamination. Office environments are generally suitable for the storage of DVDs and CDs. Allowing DVDs and CDs to become dirty or scratched damages the media and can affect the integrity of the data stored on these disks.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

For Official Use Only

PART B – Release of Information to other Government Agencies

4.11. Request by external agency

A *Request for CCTV Information (external agency) form B1203 (Attachment A)* is completed by a requesting agency and submitted to an Authorising officer who is responsible for the CCTV.

If the agency requesting the information is an agency with which Australian Border Force has an ongoing authorisation, the request can be submitted, through *the Request for CCTV Information (external agency) form* or directly to the Authorising officer who will complete the form on their behalf.

In order to complete the *Request for CCTV Information (external agency) form* on behalf of the recipient agency the following details are required:

- details of the request
- media type
- requesting agency
- requesting officer details.

The ABF officer is to complete the Authority to Disclose Immigration and Border Protection information – one off authorisation form **(TRIM ADD2018/78378)**. **Note:** This form is intended to be used internally to provide the authorisation in writing required by s44 or s45 of the Australian Border Force Act. It is not intended to be provided to external bodies accompanying disclosures. The ABF officer must be satisfied that a training course has been completed. Once complete, the ABF officer is to hand the *Authority to Disclose Immigration and Border Protection information* and *Request for CCTV Information (external agency)* forms to a CCTV operator for action.

The Authority to Disclose Immigration and Border Protection information form does not need to be completed if an ongoing authorisation is in place, authorising the disclosure to the recipient agency.

4.12. Capture information

Once the completed forms have been received, the CCTV operator is to capture the requested information and record it to the required medium (eg. DVD or printed hard copy).

The DVD/Photo is to be endorsed with the following statement and information:

- *This document is made available to [insert agency] for the purposes of investigating whether an offence has been committed against a law of the Commonwealth or a Territory or for the performance of its functions on the understanding that it will not be disclosed or further produced except when required or permitted by law.*
- person recording the information
- person provided to
- subject
- date
- security classification marking on the disk or photo.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

For Official Use Only**4.13. Release of media**

The media is to be placed in an envelope, sealed with a Australian Border Force seal and endorsed with the following information on the front of the envelope:

- person provided to
- subject
- date.

Place the envelope containing the media in the control room safe until it is collected by the requesting person or their nominated person. The identity of the requesting officer or nominated person must be verified by sighting the ABF officer's identification pass. Release of media to a nominated officer should only occur when previously advised by the requesting officer or confirmed directly with the requesting officer. The Issuing agency and identification number are to be recorded in the Control Room Release of Information Logbook (Logbook) (**Attachment B**).

4.14. Record keeping

The following details of the requested information are to be entered in the relevant Log Book (**Attachment B**):

- date of request
- format e.g. Tape, DVD, CD or photograph
- releasing officer.

Agencies that have an ongoing authorisation to disclose with ABF are still required to have their request details recorded in the relevant logbook and their request kept on file.

The Log Book reference number for the request is to be inserted into the *Request for CCTV Information (external agency)* form.

Attach the *Request for CCTV Information (external agency)* form to the *Authority to Disclose Protected Information – General form* and file under the corresponding month in the Request for CCTV Information folder.

When the recipient arrives to collect the media, complete the entry in the Release of Information Logbook (**Attachment B**) including:

- date of collection
- collector's name and agency
- collector's signature
- releasing officer.

4.15. Compliance and efficiency reporting

On a fortnightly basis, the ABF officer is to conduct a compliance check of the Release of Information Logbook (**Attachment B**) and Request for CCTV Information folder. This is to ensure that information is being correctly recorded, all details in the logbook and request forms are being recorded entirely, and that no requests are outstanding.

In the event that discrepancies are identified through this check, it must be reported to the Airport Manager. The Airport Manager then makes a determination as to whether the discrepancy should be further reported and the appropriate remedial action to be taken.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

For Official Use Only

5. Accountability and responsibilities

If ABF officers require clarification or assistance in regard to this instruction, they should contact the National Border Programme by email [S. 22\(1\)\(a\)\(ii\)@abf.gov.au](mailto:S. 22(1)(a)(ii)@abf.gov.au) or telephone: S. 22(1)(a)(ii) AEST.

The Superintendent, National Border Programme has responsibility for the preparation and dissemination of this Procedural Instruction in regards to operational policy and programme management of border clearance activities for air and sea travellers, under the Customs Act and Migration Act.

The Director, Traveller Policy Advice and Support section has responsibility for preparation and dissemination of the Policy Statement in relation to this Procedural Instruction.

6. Statement of Expectation

This Procedural Instruction under the PPCF sets out guidance and directions to workers on how to implement the Department's policy.

It is expected that all workers who are subject to this Procedural Instruction will have due regard to it and will only depart from it if:

- a) the departure is reasonable and justified in the circumstances;
- b) all risks have been considered; and
- c) approval has been sought and responsibility accepted for documenting the justification for the decision.

Workers are required to comply with all reasonable and lawful directions contained in this Procedural Instruction. Failure to comply with a direction may be considered a breach of the Australian Public Service Code of Conduct (for APS employees) or the *Professional Standards Secretary's Direction* under section 55 of the *Australian Border Force Act 2015* (for non-APS employees).

All records created as a result of this procedure must be managed in accordance with the Records Management Policy Statement. Records created as a result of this policy/procedure must be saved in TRIM RM8 or an approved business system.

7. Related Framework documents

This instruction must be read in conjunction with the following documents:

7.1. Policy Statement

[TT-2983] Border Clearance

7.2. Procedural Instructions

[TI-743] Airport CCTV – Data Security Classification

Released by Department of Home Affairs
under the Freedom of Information Act 1982

For Official Use Only

8. References and legislation

8.1. Australian Border Force Act 2015

This Act is important in the context of this instruction, particularly:

- Section 44 – Disclosure to certain bodies and persons
- Section 45 – Disclosure in accordance with agreements

8.2. Freedom of Information Act 1982

An Act to give to members of the public rights of access to official documents of the Government of the Commonwealth and of its agencies.

8.3. Crimes Act 1914

This Act sets out the requirements relating to Offences against the Commonwealth.

- Section 70 – Disclosure of information by Commonwealth officers.

9. Consultation

9.1. Internal consultation

The following internal stakeholders were consulted in the development of this Procedural Instruction:

- Integrity and Professional Standards, Integrity and Professional Standards Branch
- FOI Privacy and Records Management Branch, Records Management Section
- Traveller Policy Branch, Traveller Policy Advice and Support Section.

9.2. External consultation

No external consultation.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

For Official Use Only**10. Document details**

BCS Category/Function	Trade & Traveller Clearance Management
BCS Sub-Category/Sub-Function	Passenger and Crew Processing
Period of Effect	Three years from date of original approval.

10.1. Document change control

Version number	Date of issue	Author(s)	Brief description of change
1.0	17 May 17	s. 22(1)(a)(ii)	Update of document into PI.
1.1	30 Jan 18	s. 22(1)(a)(ii)	Cleared PPCF Quality Assurance.
1.2	21 Feb 18	s. 22(1)(a)(ii)	Reviewed for SES approval.
1.3	22 May 18	s. 22(1)(a)(ii)	Converted to Home Affairs template and reviewed for SES approval.

10.2. Approval

Approved by:	Don SMITH Commander ABF Governance
Approved on (date):	21 May 2018

Released by Department of Home Affairs
under the Freedom of Information Act 1982

For Official Use Only

11. Appendices

11.1. Attachment A – B1203 – Request for CCTV information (external agency)

(Available on Department of Home Affairs website)

FREEDOM OF INFORMATION ACT		PRIVACY ACT		AUSTRALIAN BORDER FORCE ACT	
If a request under the FOI Act is received for access to footage released in response to this request, or an extract of, please consult our FOI Coordinator in the Department of Immigration and Border Protection FOI section.		The provisions of the Privacy Act should be complied with by anyone handling personal information contained within the footage released in response to this request.		Any information that may be disclosed by ACBPS in response to this request may be subject to Part 6 of the Australian Border Force Act 2015.	
Request For CCTV Information (external agency)					
Urgency of Request: Please tick one of the following Routine ☐ (action within 3 Days) Priority ☐ (action within 1 Day) Immediate ☐ (action within 2 hours)					
Details of Request					
Date of Incident & Location					
Flight No.					
Alert No. (if applicable)					
Passenger name (if applicable)		First Name		Last Name	
Reason for Request					
Media Format Required (please tick) Note: all images and footage are security classified as Protected. Changing this classification is a security breach.					
DVD copy of Digital Video Footage	☐ Number of copies:	Photograph digital video image	☐ Number of copies:		
Photograph hard copy	☐ Number of copies:	Emailing of digital video	☐ Number of copies:		
Emailing of digital photograph	☐ Number of copies:		☐ Number of copies:		
Requesting Officer			Collecting Officer (if different to requesting officer)		
Full Name				Full Name	
Agency				Agency	
ASIC/Badge No.				ASIC/Badge No.	
Contact Phone No.				Contact Phone No.	
Signature				Signature	
Officer of Customs (APS 6 or above) - Please note that any disclosure of information by an officer within the Department of Immigration and Border Protection in response to this request must comply with Part 6 of the Australian Border Force Act 2015.					
Full Name		Title and contact Phone No.			
Signature		Date		/ /	

B1203 (JUL 15)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

11.2. Attachment B - Control Room Release of Information Log Book

S. 47E(d)

11.3. Attachment C –Sample label template

~~PROTECTED~~

 **Australian
BORDER FORCE**

Recipient: _____
Subject: _____

Log Reference No: _____
Task No. _____

Disc _____ of _____
Date of Footage _____
Date of Release _____

CCTV FOOTAGE

This disc is made available to the recipient for the performance
of the recipient's functions in investigating whether an offence
has been committed against a law of the Australian
Commonwealth or an Australian State or Territory

This information is disclosed on the understanding that it will not
be used or further disclosed except for the purpose for which it
was provided by Australian Border Force or otherwise as
required or authorised by law.

~~PROTECTED~~

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*



~~PROTECTED~~

Airport CCTV - Incident response

Procedural Instruction

This instruction provides Closed Circuit Television (CCTV) processes to follow in instances of Passenger Analysis Clearance Evaluation Alarm (PACE) alerts or duress alarms triggering, as well as managing general surveillance activities at airports.

Approval Date	13 June 2018
Date of Review	13 June 2019
Contact	S. 22(1)(a)(ii) @abf.gov.au
Document ID (PPN)	TI-746
TRIM Reference	OPD2017/203842

Released by Department of Home Affairs
under the Freedom of Information Act 1982

~~PROTECTED~~

Table of Contents

1. Introduction

1.1. Background

2. Scope

2.1. In Scope

2.2. Out of Scope

3. Glossary

4. Procedural Instruction

5. Accountability and responsibilities

6. Statement of Expectation

7. Related Framework documents

7.1. Policy Statement

7.2. Procedural Instructions

8. References and legislation

8.1. Australian Border Force Act 2015

9. Consultation

9.1. Internal consultation

9.2. External consultation

10. Document details

10.1. Document change control

10.2. Approval

3

3

3

3

3

4

4

4

5

5

6

6

6

7

7

7

7

7

7

7

8

8

8

S. 47E(d)

1. Introduction

1.1. Background

It is important to the operation of Closed Circuit Television (CCTV) at airports that response to major incidents is handled in a consistent and comprehensive manner. Inadequate incident response handling policies and procedures may result in incorrect actions being undertaken in the event of an incident, possibly delaying resolution and interfering with ABF ability to meet CCTV objectives, service level charters and border security requirements. The incidents included in this scope are reactions to Departmental systems and s. 47E(d)

2. Scope

2.1. In Scope

This procedural instruction provides CCTV processes to follow in instances of travellers of interest, duress alarm activation or general surveillance activities at airports.

This procedural instruction applies to staff in the Aviation and Maritime environments.

2.2. Out of Scope

This procedural instruction does not cover how to operate the CCTV system.

Clearance of travellers and/or goods under the *Customs Act 1901* (Customs Act).

3. Glossary

Table 1 – Common terms and definitions used in this instruction

Term	Acronym (if applicable)	Definition
AFP Operations Coordination Centre	AOCC	AOCC provides a centralised monitoring, initial response and coordination and communications support service for the AFP's national and international activities.
Australian Border Force	ABF	The Australian Border Force is an agency within the Home Affairs portfolio responsible for offshore and onshore border control enforcement, investigations, compliance and detention operations in Australia
Australian Border Force officer	ABF officer	An ABF officer is an Immigration and Border Protection worker (see section 4 Australian Border Force Act) authorised to perform border clearance duties.
Closed Circuit Television	CCTV	Is a system of video monitoring at Australia's international airports and seaports.

s. 47E(d)

4. Procedural Instruction

s. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

S. 47E(d)

5. Accountability and responsibilities

If ABF officers require clarification or assistance in regard to this instruction, they should contact the National Border Programme by email S. 22(1)(a)(ii) @abf.gov.au or telephone: S. 22(1)(a)(ii) AEST.

The Superintendent, National Border Programme has responsibility for the preparation and dissemination of this Procedural Instruction in regards to operational policy and programme management of border clearance activities for air and sea travellers, under the Customs Act and Migration Act.

The Director, Traveller Policy Advice and Support section has responsibility for preparation and dissemination of the Policy Statement in relation to this Procedural Instruction.

6. Statement of Expectation

This Procedural Instruction under the PPCF sets out guidance and directions to workers on how to implement the Department's policy.

It is expected that all workers who are subject to this Procedural Instruction will have due regard to it and will only depart from it if:

- a) the departure is reasonable and justified in the circumstances;
- b) all risks have been considered; and
- c) approval has been sought and responsibility accepted for documenting the justification for the decision.

Workers are required to comply with all reasonable and lawful directions contained in this Procedural Instruction. Failure to comply with a direction may be considered a breach of the Australian Public Service Code of Conduct (for APS employees) or the *Professional Standards Secretary's Direction* under section 55 of the *Australian Border Force Act 2015* (for non-APS employees).

All records created as a result of this procedure must be managed in accordance with the Records Management Policy Statement. Records created as a result of this policy/procedure must be saved in TRIM RM8 or an approved business system.

7. Related Framework documents

This instruction must be read in conjunction with the following documents:

7.1. Policy Statement

[TT-2983] Border Clearance

7.2. Procedural Instructions

[BC-536] Arrival, immigration clearance at airports and seaports

8. References and legislation

8.1. Australian Border Force Act 2015

This Act is important in the context of this instruction, particularly:

- Section 44- Disclosure to certain bodies and persons
- Section 45 – Disclosure in accordance with agreements.

9. Consultation

9.1. Internal consultation

The following internal stakeholders were consulted in the development of this Procedural Instruction:

- Integrity and Professional Standards, Integrity and Professional Standards Branch
- FOI Privacy and Records Management Branch, Records Management Section
- Traveller Policy Branch, Traveller Policy Advice and Support Section.

9.2. External consultation

No external consultation.

10. Document details

BCS Category/Function	Trade & Traveller Clearance Management
BCS Sub-Category/Sub-Function	Passenger and Crew Processing
Period of Effect	Three years from date of original approval.

10.1. Document change control

Version number	Date of issue	Author(s)	Brief description of change
1.0	17 May 17	s. 22(1)(a)(ii)	Update of document into PI
1.1	11 July 17	s. 22(1)(a)(ii)	Cleared PPCF Quality Assurance
1.2	16 Feb 18	s. 22(1)(a)(ii)	Reviewed for SES approval
1.3	20 April 18	s. 22(1)(a)(ii)	Converted to Home Affairs template and reviewed for SES approval

10.2. Approval

Approved by:	Don SMITH Commander ABF Governance
Approved on (date):	13 June 2018

Released by Department of Home Affairs
under the Freedom of Information Act 1982



Freedom of Information Request – FA 25/12/01786

s. 33(a)(i), s. 47E(d)

The Department's policy in relation to the holding of any vision captured by the CCTV cameras within specified areas of the Perth International Airport

In Australia, there is no single, mandatory, across-the-board legal retention period for CCTV footage. However, industry guidelines and standards, particularly AS 4806.1-2006 (Closed Circuit Television Management and Operation), recommend a minimum retention period of 31 days.

Notes:

1. Source: Department of Home Affairs (internal documents)

Caveats:

- This information is provided for the specific purpose of this request.