Australian Government
Department of Home Affairs

OFFICIAL: Sensitive

Digital Device Examination

Procedural Instruction

Document ID (PPN)	BE-6185
TRIM record number	ADD2019/2716067
BCS Function	Border Enforcement
Document owner	Commander Tactical Capability Branch
Approval date	23 July 2020
Document Contact	Superintendent Special Technical, Tactical Capability Branch s. 22(1)(a)(ii)

OFFICIAL: Sensitive

Table of Contents

1. Purpose

The Australian Border Force (the ABF) is the operational enforcement arm of the Department of Home Affairs (the Department). Through the exercise of certain statutory powers, Border Force Officers (BFOs) may examine electronic devices in different operational domains.

The ABF ensures that BFOs are appropriately trained, equipped and operationally capable to perform effectively across operational domains, including the manual examination of electronic devices.

The powers of BFOs to conduct examinations are mainly found in the *Customs Act 1901* (the Customs Act), the *Migration Act 1958* (the Migration Act) and the *Maritime Powers Act 2013* (the Maritime Powers Act).

This Procedural Instruction provides an outline of the Digital Device Examination capability used by the Australian Border Force (ABF) in support of its border protection function. The document describes the standards and governance framework for the capability.

2. Scope

This Procedural Instruction provides guidance on the examination of electronic devices by BFO's utilising the dedicated Digital Device Examination (DDE) hardware and software.

Only mobile devices and removable data storage devices are to be examined using the DDE capability.

This document provides general guidance only and is not intended to summarise or replicate all applicable legislative requirements. As a result, it must be read as subject to any applicable laws. It should also be read in conjunction with the *Electronic Device Examination* Policy Statement (BE-6168).

3. Procedural Instruction

3.1. Introduction

The ABF examines electronic devices through its electronic device examination capability framework. This includes the ABF's ability to examine electronic devices through its DDE capability, through referral for more specialised examination by Digital Forensics Investigators (DFI's) or a third party or by manual examination.

The examination of electronic devices may:

- Potentially compromise electronic evidence, affecting its admissibility
- Risk overlooking relevant evidential material
- Hinder the successful outcome of the Department of Home Affairs (the Department) objectives and/or decisions
- Result in failure to bring an investigation to an appropriate conclusion
- Cause damage to equipment or data resulting in civil claims against the Department and
- Risk damage to the ABF's organisational reputation.

Compliance with the ABF's electronic device examination capability framework limits these risks.

3.2. Legislative Authority

3.2.1. Examining Devices

The relevant statutory frameworks empower Officers to conduct examinations for prescribed purposes. Officers should be aware of the possibility that when they conduct an examination for one purpose, they may uncover material that is relevant to other purposes - and that this may enliven other statutory powers and obligations. Officers may examine devices subject to Customs control using section 186 of the *Customs Act 1901* (the Customs Act).

In certain circumstances Officers may examine electronic devices using section 252 of the *Migration Act 1958* (the Migration Act).

In the marine environment Officers examine devices using section 63 of the *Maritime Powers Act 2013* (the Maritime Powers Act). Officers must ensure that powers permitted under the Maritime Powers Act are exercised only in accordance with Part 2 of the Maritime Powers Act.

Given the operational flexibility of the section 186 Customs Act power and the limitations of the section 252 Migration Act power, it is the ABF's position that examination of electronic devices using the DDE will be undertaken utilising the section 186 Customs Act power as the primary statutory authority, except in marine environments. The use of other statutory powers is available to Officers following a section 186 examination.

The examination of electronic devices resulting from warrant activity and any subsequent action must comply with the respective search warrant legislative authority.

Statutory authority allows the use of photographs being taken and in, limited circumstances, video recording of the manual examination of electronic devices. This can only occur if it constitutes examination of the goods under section 186 of the Customs Act.

3.2.2. Questioning

BFO's may question people regarding the contents of their electronic devices under:

- section 195 of the Customs Act
- section 192 of the Migration Act, and
- section 57 of the Maritime Powers Act.

Note that the above powers are limited and querying the contents of a device or requesting a passcode, PIN or PUK need to align with the specified circumstances in which the powers can be used, If questioning does not come within these powers, BFOs must not suggest that people are compelled to respond.

3.2.3. Copying Data

"Copy" " is not defined in either the Customs Act, Migration Act or the Maritime Powers Act. For the purposes of this instruction, "copy" means to make a similar or identical version or to reproduce a document. It is considered that a device constitutes a document for the purposes of the Customs Act, Migration Act or the Maritime Powers Act. It is also considered that the use of a photograph or video record (if applicable) is a method of taking a copy.

An Officer may make a copy of electronic records or documents subject to customs control, or an extract may be taken:

- By photocopying the document or a part of the document, or
- By photographing the document or a part of the document (this does not include a video recording), or
- By electronically scanning the document or a part of the document, or

- By making an electronic copy of information contained in the document or a part of the document, or
- By making a written copy of information contained in the document or a part of the document, observed during the examination of electronic device.

BFO's can copy electronic records or documents from electronic devices using section 252 of the Migration Act, subject to certain circumstances. This includes the photographing **and video recording** of information displayed on a device and the creation of written records of data observed during the examination of electronic devices.

In the marine environment, BFO's may copy electronic records or documents from electronic devices using section 65 of the Maritime Powers Act. Officers must ensure that powers permitted under the Maritime Powers Act are exercised only in accordance with Part 2 of the Maritime Powers Act.

An extraction or acquisition of a mobile device undertaken for purposes of an examination, **is not a copy** for the purposes of the relevant statute. Only when the conditions for the copy are met and a copy is made to another storage medium that a COPY is said to exist.

BFO's must understand that, 186A powers may only arise once an examination undertaken as part of section 186 Customs Act has been conducted, and as a result of that examination, an Officer is satisfied that the conditions in paragraph 186A(1)(b) have been met – a copy is then made to a separate storage medium. If a copy is made without s186A being complied with, the copy will be unlawful.

BFO's are to comply with the Department's procedures to meet the requirements and obligations under the *Privacy Act 1988* (the Privacy Act) when making copies of any document/s.

3.3. Equipment

The examination of devices using the DDE capability must only occur using approved equipment. This equipment is verified and maintained to ensure it delivers a consistent examination outcome. No unauthorised equipment is to be connected to the deployed examination computer system.

Specialised software applications on dedicated computer systems are deployed to enable trained and authorised officers to examine mobile devices and removable storage media in support of their operational duties. The requisite training is outlined below at 3.4

This suite of approved equipment includes:

- A dedicated laptop or workstation utilising a customised Standard Operating Environment (SOE)
- A software application package for the examination of mobile devices and removable storage media, and
- A range of software tools for the examination of removable storage media, comprising software :
    - To scan files for the presence of skin tone of a person and key words of interest. As an automated tool, it can reduce the time needed to examine devices and media when compared to manual techniques, while increasing the likelihood of detecting material of interest.
    - To recover deleted material not accessible by the Windows operating system and regular software applications.
    - To preview data and acquire data (evidence) in a forensically sound manner by creating copies of data without making changes to the original evidence.
    - A selection of media players able to play a range of video file types.

The computer systems, laptop or workstation have write blocking software installed to prevent any changes to the data on the device and ensure the integrity of the examination product.

3.4. Training

Only Officers who have been assessed as competent under the approved DDE training may examine electronic devices or copy electronic records or documents using the DDE capability. Any BFO with a genuine need-to-know may review acquired, extracted or copied electronic records or documents in the course of their duties.

3.5. Examination

Consistent with the *Policy Statement - Electronic Device Examination* (BE-6168), the ABF utilises an escalation approach to examine electronic devices. This usually results in devices being examined by the DDE capability before any other examination capability is considered. In some instances another examination approach is conducted first, usually because:

- The DDE capability is not available, either because the hardware and software is not available, or because no trained and authorised officers are available, or
- The electronic device cannot be examined by the DDE capability.

Keeping in mind that an Officer may arrange for another BFO or other person having the necessary experience to do whatever is reasonably necessary to **permit the examination** of the goods concerned – subsection 186(2) of the Customs Act.

In instances where an officer or work area decides to use another examination approach when the DDE capability could be used the officer or work area must;

- Record the reason for non-compliance with the *Policy Statement - Electronic Device Examination* (BE-6168), and
- Conduct the other examination consistent with the requirements of the relevant Procedural Instruction.

Once taken for examination, Officers must not return electronic devices until the examination is complete.

Regardless of the intended examination method the owner of the electronic device must not be allowed to interact with the device from the time the Officer has decided to examine the device to the time the Officer has completed their examination and, if necessary, copied data from the device.

For detailed instructions for the examination of electronic devices see *Standard Operating Procedure – Use of Digital Device Examination to examine electronic devices* (BE-6197).

If it is decided that a copy of data or document/s is to be made, following a DDE examination, the electronic device must not be returned to the owner until the copy has been made.

For detailed instructions for the copying of electronic records or documents see *Standard Operating Procedure – Digital Device Examination – Copying, transfer and storage of data* (BE-6198).

s. 22(1)(a)(ii)

[redacted]

s. 22(1)(a)(ii)

[redacted]

3.7. Record Keeping

It is critical that officers make contemporaneous notes in a form that enables them to account for continuity of the electronic devices seized and any copies made, compile reports, statements, conduct interviews and, if required, be used as evidence in court. Contemporaneous notes are to be made in an officer's official notebook and on an approved examination form.

All examinations by the DDE capability is to be recorded on an approved Digital Device Examination Form and in Baggage Action General Statistics (BAGS), where available. If BAGS is not available the examination is to be recorded in an Electronic Device Examination Register (see *Supporting Material – Electronic Device Examination Forms (BE-6199*). There is to be a separate examination form for every device examined (note: components of a device can be included on the same form, for example mobile device handset, SIM card, removable storage card etc).

Any copy made of data or document/s resulting from a DDE examination is to be recorded on the examination form. These details must include, but are not limited to, the name of the officer who made the copy, the date the copy is made, the name of the copied data, the statutory power exercised to make the copy, the reasons for making the copy and the transfer of any copied data and detained or seized goods. All copies made must also be recorded in the examination register.

This record keeping is in addition to currently existing local and national arrangements, such as in National Intelligence System (NIS).

s. 22(1)(a)(ii)

[redacted]

s. 22(1)(a)(ii)

4.1. Statement of Expectation

4.1.1. Directions

The APS *Code of Conduct* states that 'an APS employee must comply with any lawful and reasonable direction given by someone in the employee's Agency who has authority to give the direction' (subsection 13(5) of the *Public Service Act 1999*).

Failure by an APS employee to comply with any direction contained in a PPCF document may be determined to be a breach of the APS *Code of Conduct*, which could result in sanctions up to and including termination of employment, as set out in subsection 15(1) of the *Public Service Act 1999*.

The Secretary's *Professional Standards Direction*, issued under subsection 55(1) of the *Australian Border Force Act 2015*, requires all IBP workers who are not APS employees (such as contractors or consultants) to comply with any lawful and reasonable direction given by someone in the Department with authority to issue that direction.

Failure by an IBP worker who is not an APS employee to comply with a direction contained within this document may be treated as a breach of the *Professional Standards Direction*, which may result in the termination of their engagement under section 57 of *the Australian Border Force Act 2015*. Non-compliance may also be addressed under the terms of the contract engaging the contractor or consultant.

4.1.2. Policy, Guidelines and Recommendations

For all other provisions of PPCF documents, the Secretary and the Commissioner expect all IBP workers to:

- Consider whether a proposed departure from any provision set out in a PPCF document is reasonable and justified in the circumstances;
- Consider the risks of departing from any provision set out in a PPCF document;
- Be responsible and accountable for the consequences of departing from, or not adhering to the content of, all PPCF documents, including where such departure or non-adherence results in a breach of any legal or other obligations which lead to adverse outcomes for the Department;
- Be responsible for documenting the reasons/justification for their decision to depart from, or not adhere to, any PPCF document.

4.1.3. Exercise of Legislative Powers and Function

IBP workers who make decisions or who exercise powers or functions under legislation have a duty to make these decisions or exercise these powers or functions in accordance with the requirements of the legislation and legal principle.

4.1.3. What happens if this Procedural Instruction is not followed?

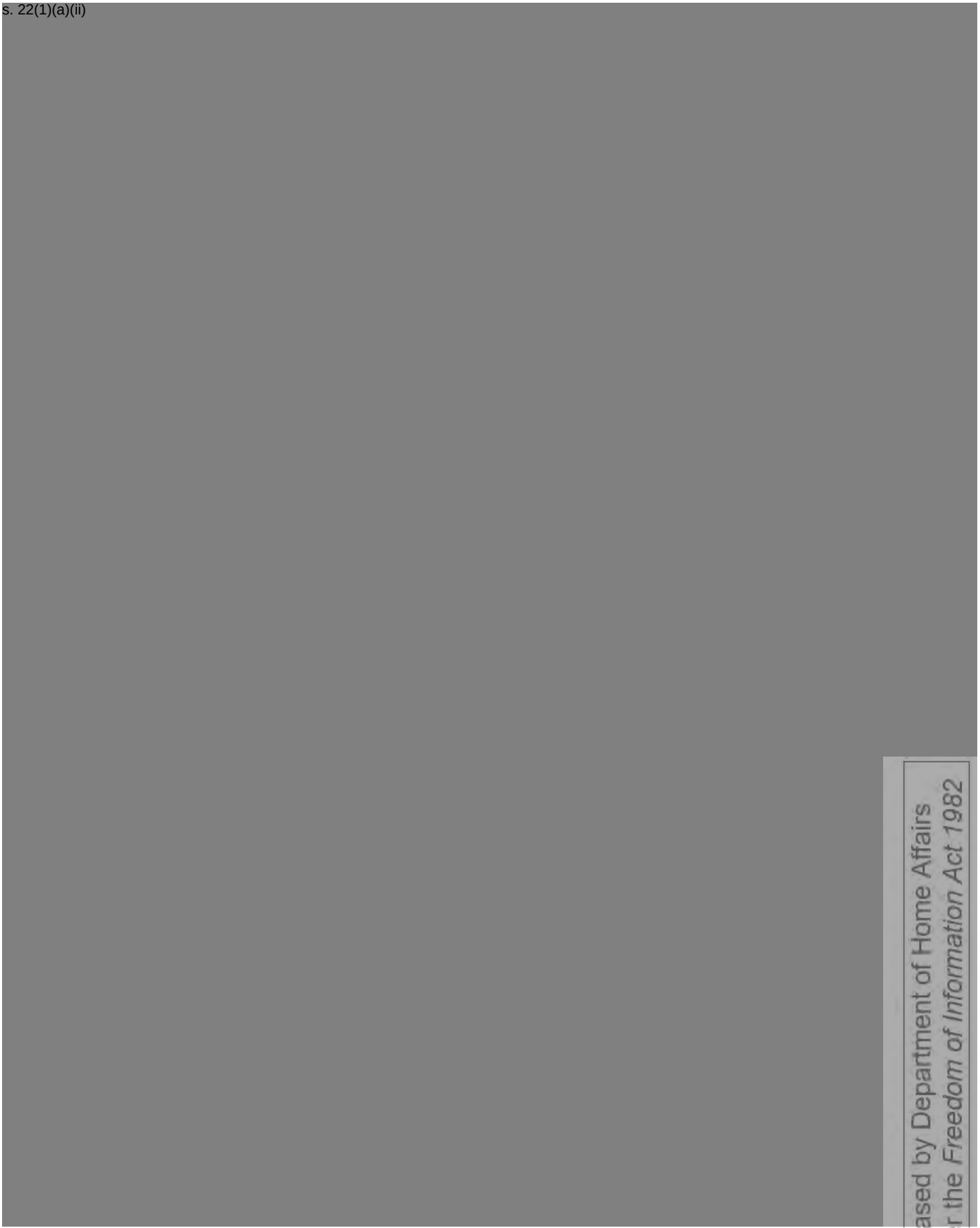
Failure to comply with a direction contained in this document may constitute a breach of the *APS Code of Conduct*, and may result in a sanction, up to and including termination of employment, being imposed under subsection 15(1) of the *Public Service Act*.

For IBP workers who are not APS employees, failure to comply may constitute a breach of a direction under section 55 of the *Australian Border Force Act 2015*, and may result in the termination of their engagement under section 57 of that Act. Non-compliance may also be addressed under the terms of the contract engaging the IBP worker.

s. 22(1)(a)(ii)

s. 22(1)(a)(ii)

s. 22(1)(a)(ii)



s. 22(1)(a)(ii)

s. 22(1)(a)(ii)

s. 22(1)(a)(ii)

s. 22(1)(a)(ii)

s. 22(1)(a)(ii)

s. 22(1)(a)(ii)