Use of Digital Device Examination to examine electronic devices

Standard Operating Procedure

Document ID (PPN)	BE-6197
TRIM record number	ADD2019/2731340
BCS Function	Border Enforcement – Enforcement Operations Management
Document owner	Commander Tactical Capability Branch
Approval date	23 July 2020
Document Contact	Special Technical, Tactical Capability Branch, Close Support Command – s. 22(1)(a)(ii)

Table of Contents

1. Purpose

This Standard Operating Procedure (SOP) must be read in conjunction with *Policy Statement – Electronic Device Examination* (BE-6168) and *Procedural Instruction – Digital Device Examination* (BE-6185) and all associated SOPs and Supporting Material and applicable legislation.

These procedures will ensure that any activity undertaken meets accepted best practice for Digital Device Examination (DDE) and any legislative requirements.

DDE activities must only be undertaken by appropriately trained and skilled DDE examining officers using dedicated tools and rigorous procedures in accordance with legislation and electronic evidence handling procedures so as to be admissible as evidentiary material in a court of law.

Examination of electronic devices should not be undertaken by unqualified/untrained persons as such actions can:

- Potentially compromise electronic evidence affecting its admissibility
- Hinder the successful outcome of the Department of Home Affairs (the Department) objectives
- Cause damage to equipment or data resulting in civil claims or litigation against the Department
- Result in failure to bring an investigation to an appropriate conclusion
- Risk damage to the Department's reputation.

This SOP supports the Department's ability to demonstrate the reliability of the electronic evidence.

2. Scope

This SOP applies to all examinations of electronic devices by the Australian Border Force (the ABF) utilising the Digital Device Examination equipment and capability.

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

3. Standard Operating Procedure

Prior to examining a device the DDE examining officer **must** consider

- The ABF Statutory powers for the examination, including any legislated time limitations
- The purpose of the examination, including consultation with the client if necessary
- Whether the DDE examining officer possesses the necessary resources and tools to facilitate the examination, including
    - Software
    - Hardware
    - Cables, and/or
    - Device documentation
- The operational environment the examination is occurring in. If the device belongs to a traveller the officer should consider whether the device should be retained for examination so that the passenger is not unnecessarily delayed. The examination length and comprehensiveness **must** be determined by the operational need, not by external factors such as departing flights.

3.1 Device Identification

DDE Examining officers must only examine mobile devices and removable data storage devices that they have been trained to examine.

DDE Examining Officers encountering devices that they cannot identify, do not know how to operate or are experiencing difficulty in examining should consider requesting these devices be examined by Digital Forensics.

3.2 Data Preservation and Acquisition

All examinations of mobile devices and removable data storage devices **must** be undertaken using DDE hardware and software to ensure the integrity of data and electronic evidence is maintained to the highest level possible.

Ensure appropriate steps are taken to secure electronic devices and electronic records, as follows:

- A Digital Device Examination **must** be attempted before a manual examination is considered
- Mobile devices **must** be isolated from the mobile communications network (aeroplane/airplane/flight mode turned on, SIM card removed, faraday bag and/or WIFI and Bluetooth disconnected) prior to any examination
- SIM cards **should** be removed and extracted separately
- Removal of the SIM card is only mandatory if the device cannot be isolated from the network by activating 'Flight Mode' on the device itself.
- Write protection **must** be ensured for any connected removable data storage device
- Consider acquiring data from removable storage separately
- Should there be any indication of third party encryption software being installed or encryption being part of the operating system (e.g. encrypted volume) or anti-forensics techniques being installed such as destructive devices and data wiping software, the device must be examined by Digital Forensics.
- If the device needs to be powered-down, consider whether it will be possible to unlock the device once power is restored. If it is not possible to unlock the device then an examination using DDE equipment **must** be attempted.

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

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

3.4. Record Keeping

It is critical that DDE examining officers make contemporaneous notes in a form that enables them to compile reports, statements, conduct interviews and, if required, be used as evidence in a Court of Law. Contemporaneous notes are to be made in a DDE examining officer's official notebook and on an approved Digital Device Examination Form.

If a DDE examining officer uses an ABF statutory power in relation to the examination of an electronic device, an official record **must** be made with details of the reasons that led them to form their state of mind and the statutory power used, such as subparagraph 186A(1)(b)(i) of the *Customs Act 1901* (the Customs Act).

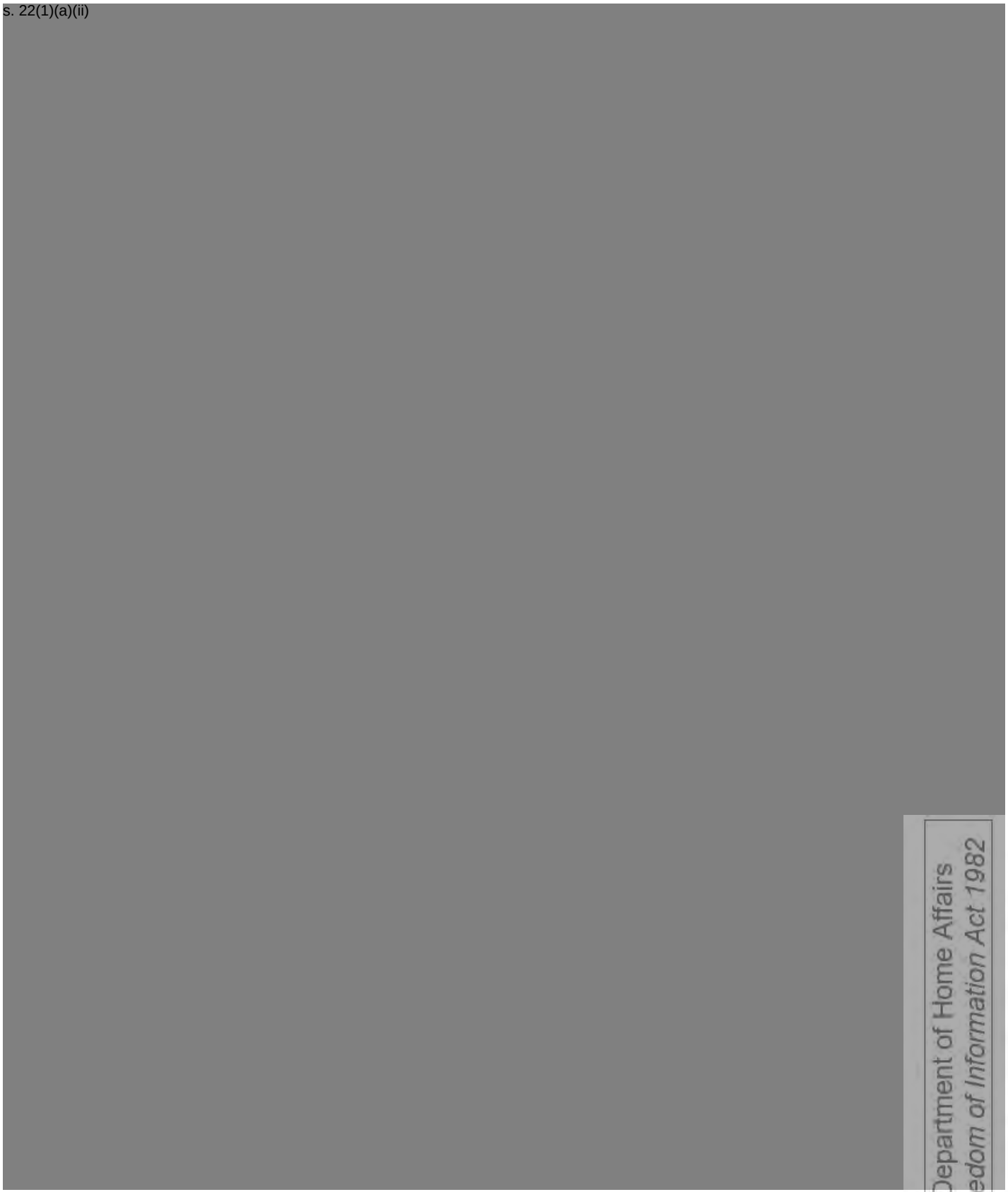
For the purposes of DDE **all** examinations **must** be recorded contemporaneously on an approved *Digital Device Examination Form* and in Baggage Action General Statistics (BAGS) (where available). This form will follow the approved form in *Supporting Documentation – Electronic Device Examination Forms (BE-6199)*.

If BAGS is not available the examination is to be recorded in an Electronic Device Examination Register (see *Supporting Material – Electronic Device Examination Forms*). A separate *Digital Device Examination Form* is to be completed for each individual device.

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

[redacted]

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



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 BP worker who is not an APS employee to comply with a direction contained in a PPCF 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.

4.1.4. What happens if this SOP 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)

[redacted]

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

[redacted]

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

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

[redacted]

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

Attachment C – Consultation

1.1. Internal Consultation

- Tactical Capability Branch, Close Support Command
- Operational Capability Branch, Major Capability Division
- Cyber Risk Services Branch
- ICT Division
- Integrity and Professional Standards
- Privacy and Information Disclosure Section
- PPCF Section
- Legal Group

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

[redacted]

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