Seizure of Contraband Cellular Telephones

Electronic communication devices such as contraband cellular telephones may contain criminal evidence and/or vital threat information. Devices must be handled correctly in order to provide the best chances of exploitation and to maintain the integrity of the evidence for use in court. Any activity or function performed on a contraband cellular telephone may be logged by the device and then become discoverable in court proceedings. It is imperative that all handling and any manual examination of contraband cellular telephones be properly logged and reported. The office of the Inspector General (OIG) recommends that untrained staff only perform the most basic functions upon the seizure of contraband cellular telephones. OIG recommends that manual examinations of contraband cellular telephones only be conducted by trained staff, and only when necessary for institutional security.

I. **Seizure of Cellular Telephones (Passwords)** — any staff member who seizes a cellular telephone should attempt to identify and document any passwords, unlock codes, or unlock patterns.

   A. Possible methods for obtaining passwords, codes, or patterns include: asking the inmate; searching the cell/area for written passwords, codes, or patterns; or talking to other inmates.

   B. Untrained staff SHOULD NOT attempt to guess unlock codes by entering random numbers or patterns. Multiple unsuccessful unlock attempts may limit later efforts by trained staff.

   C. DO NOT clean or wipe off the screen of contraband cellular telephones, as this may interfere with forensic techniques for unlocking the device.

II. **Seizure of Cellular Telephones (On/Locked)** — any seized device, which is already powered on, may contain volatile encryption keys and SHOULD NOT be turned off. The device must be isolated from all networks as soon as possible to prevent the device from receiving any signals, which may cause the device to overwrite all stored data. The device can be isolated from network by putting the device into “Airplane Mode” or removing the Subscriber Identity Module (SIM) card.

   A. **“Airplane Mode”** — if the staff member seizing the contraband cellular telephone is comfortable doing so, they may place the device in “Airplane Mode” utilizing one of the following techniques:

      1. **Android** — android devices can be placed in airplane mode using one of the following methods:

         a. Hold the power/sleep button for a couple of seconds until a menu of options appears. Select “Airplane Mode” if it appears as one of the options; or

         b. While the device screen is active, swipe down from the top of the screen to reveal a list of options/icons. Select the airplane

icon from the list. Swiping left or right may reveal more options if the airplane icon is not immediately visible.

2. **Apple iPhones or iPads** — "Airplane Mode" can be accessed and enabled on iPhones or iPads utilizing one of the two following methods:

   a. **iPhone 8 or earlier (Home Button)** — while the device screen is active, swipe up from the bottom of the screen to reveal a list of options/icons. Select the airplane icon from the list.

   b. **iPhone X or later (No Home Button)** — while the device screen is active, swipe down from top right corner of the screen to reveal a list of options/icons. Select the airplane icon from the list.

3. If staff are unable place the phone in "Airplane Mode" or are not comfortable attempting to do so, refer to Section II.B., SIM Card Removal.

B. **SIM Card Removal** — If staff are unable to place the contraband cellular telephone in "Airplane Mode", removing the SIM card may be an option.

1. **SIM Card Underneath Battery** — Many Android devices store the SIM card underneath the removable battery.

   a. Untrained staff SHOULD NOT remove the battery from a device, which is powered on. The device should be provided to a trained staff member as soon as possible to determine the best forensic options. If a trained staff member is not immediately available, proceed to Section II.C., Physically Blocking Signals.

   b. A trained staff member will determine if other options for network isolation are available. The trained staff member will also determine the significance of the device to determine if the device should be connected to a power source, or if the battery can be removed.

2. **SIM in External Storage Tray** — if the device battery is not removable, it is likely the SIM card is stored in a small tray on the side, top, or bottom of the device.

   a. Insert a small paperclip into the hole of the SIM storage tray to eject it. Remove the SIM card.

   b. Tape the SIM card to the back of the device, OR place the SIM card in a small, properly labeled bag or envelope and ensure it remains with the device from which it was removed.

C. **Physically Blocking Signals** — if staff are unable to place the device in "Airplane Mode" or remove the SIM card following the above steps, the device may be physically prevented from receiving a signal utilizing one of the following methods.

1. **Aluminum Foil** — an electronic communication device may be prevented from receiving a signal by wrapping the device in multiple layers of aluminum foil.

2. **Metal Can** — an electronic communication device may be prevented from receiving a signal by placing the device in a metal can, such as an arson can. (Arson cans are available for purchase from evidence collection suppliers.)

3. **Faraday Bag** — an electronic communication device may be prevented from receiving a signal by placing the device in a Faraday bag. (Faraday bags are available from numerous online retailers.)

III. **Seizure of Cellular Telephones (On/Unlocked)** — any seized device, which is on and unlocked, may contain volatile encryption keys and SHOULD NOT be turned off or allowed to go to sleep/become locked.

A. **Preventing Locking/Sleep Mode** — any staff member who seizes an electronic communication device, which is on and unlocked should prevent the device from locking or going to "sleep".

1. Touch the screen of the device, without opening new windows or programs, every few seconds or if the screen becomes dimmed.

2. If comfortable doing so, place the device in "Airplane Mode" in accordance with Section II.A.

3. IMMEDIATELY contact a trained staff member and transfer the device to the trained staff member without allowing the device to become locked or enter sleep mode.

4. As with all phones, attempt to locate or determine any passwords or passcodes, as these may aid in the forensic examination of the device.

5. The staff member who seized the device will properly document the seizure as well as their actions related to manipulating the device

B. **Manual Examination: Unknown Importance** — if necessary for institutional security, a trained staff member may manually examine an on/unlocked device, which is of unknown importance to the OIG or other law enforcement. The trained staff member will:

1. Ensure any manual examination is conducted in a secure location away from outside interference.

2. Ensure the device is isolated from any networks prior to conducting a manual examination.

3. Properly document all steps taken during the manual examination.

4. Take photographs of the screen of the device to document any items of evidentiary value.

5. Will disable start-up or lock screen security features, if possible.

6. Will contact the OIG if the device could be of possible interest to the OIG or other law enforcement entities to determine any additional steps prior to turning off the device.

C. **Manual Examination: Known Importance** — if an on/unlocked device is known or believed to be of importance to the OIG or other law enforcement, the trained staff member will contact the OIG, prior to any manual examination, to determine the appropriate action.

IV. **Seizure of Cellular Telephones (Off)** — any device, which is off when seized, should remain off.

A. The battery and/or SIM card should be removed from the device, but should be properly maintained with the device as instructed in Section II.B.2.b.

B. As with all devices, attempts should be made to secure password, passcodes, or unlock patterns.

C. If the device is believed to be of importance to the OIG, other law enforcement, or institutional security, the phone should be transferred to a trained staff member. The trained staff member should contact OIG to determine the appropriate action.