A. Purpose:

This SOP outlines the steps to be taken when there is a request for unlocking of an Apple iPhone or Android cell phone using the Cellebrite Premium UFDR technology. Cellebrite Premium software and hardware by Cellebrite is a product that conducts a brute force attack on iPhones and supported Android devices.

The ability of Cellebrite Premium to access a phone depends on the encryption technology resident on the device.

The encryption technology found within iOS on Apple devices is built on the security of two separate processors: the Secure Enclave (SEP) and also, on some devices, the Secure Element (SE). Additionally, a principal factor in the nature of the brute force is whether the device is in the Before First Unlock (BFU) or After First Unlock (AFU) state. Devices that are in the After First Unlock state have been unlocked at some point in the past since being turned on. Regardless of how long the phone has been running, if it has maintained power continuously since the first unlock, it is in the AFU state. This is different from a phone that may have been powered down for storage after being seized for evidence. The large majorities of evidentiary phones are in the BFU state, as they have been powered down and stored or have lost their battery charge and need to be recharged prior to analysis.

Before iOS 10.3.2, the speed of the Cellebrite Premium brute force was always the same whether the phone was in the AFU or BFU state. The anticipated maximum brute force time for a 4 digit passcode was about 25 minutes, and the maximum brute force time for a 6 digit passcode was about 2 days with approximately 1 million attempts. When iPhones 6 was introduced to the market, these came with the "Secure Element" that is embedded in the NFC chip. This was used for secure communication with the device and Apply Pay terminals. The use of this Secure Element started with iOS 10.3.2, on devices that are equipped with the NFC chip. The use of the SE is not automatic for new users of iPhone 6 or later models. After the device is first set up for use, the SE is tested for at least 2 weeks prior to activating live. During this two week trial period, the behavior of the Cellebrite Premium is the same as before. However, if the evidence phone has been in use for longer than the two week period, which is the majority of the devices, the brute force speed is affected. The brute force time is increased due to the SE now being included in the iOS authentication process. Once the two week grace period has passed, this new authentication mechanism can be referred to as an "SE-Bound Passcode".

B. Definitions/Abbreviations:

- SEP – Secure Enclave

- SE – Secure Element
- BFU – Before First Unlock
- AFU – After First Unlock
- DFU – Device Firmware Update

C. Procedure

Note: The request for this device in Justice Trax is designated as "Cellebrite Locked Device".

Apple Devices:

1. Upon receipt of the device, determine if the device is powered "on" or needs to be charged. Once the device is charged, the device should be powered "off" in BFU.

   All information regarding the device and the device lock status will be recorded on QR-CC-57 (Passcode Agent Install/Extraction Worksheet).

2. The device should be placed in Recovery mode and DFU mode.

3. Connect the device to the appropriate adapter.

4. Begin installation of the agent and start the Autonomous Brute Force detection process.

5. Remove the device from the adapter and connect to a power source.

6. Once the process is completed, the device is connected to the laptop and the Cellebrite Premium software and extraction process is initiated.

7. Save the full file system extraction to an external drive and then proceed as indicated in CC SOP-18 (Cell Phone Analysis Protocol) or CC-SOP-44 (Cell Phone Data Extraction).

Android Devices:

1. Upon receipt of the device, determine the lock status of the device.

2. All information regarding the device and the device lock status will be recorded on QR-CC-57 (Passcode Agent Install/Extraction Worksheet).

3. Determine the chipset of the android model using one of the online mobile phone assessment websites: i.e phonedb.net;gsmarena.com; phonescoop.com and/or imei.info.

4. Begin exploit and initialization for the identified model device and chipset following the on screen instructions. Ensure that the device is an approved vendor before proceeding with the method steps.

5. Connect the cable to the adapter (BE CERTAIN THAT IT IS THE ANDROID ADAPTER) and then connect the cable to the device. Follow on screen instructions.

6. Complete the extraction following the on screen instructions and save to a designated folder.

7. Save the physical extraction to an external drive and then proceed as indicated in CC SOP-18 (Cell Phone Analysis Protocol) or CC-SOP-44 (Cell Phone Data Extraction).