A. Purpose:

This SOP outlines the steps to be taken when a request for unlocking of an Apple iPhone using the GrayKey software. GrayKey software and hardware by Gray Shift is a product that installs an agent onto iPhones that are charged via a lightning cable. The lightning cable connector was introduced by Apple in September of 2012. The first compatible device using the lightning cable connector was the iPhone 5 series.

GrayKey is used to brute force an iOS passcode depending the following factors: iOS Device Model, iOS version, current state of the device (before first unlock versus after first unlock) and how long that the iPhone has been in use.

GrayKey technique will have three separate phases:

- Initial access via the USB lightning cable, if possible enable the Airplane Mode and disable WiFi.
- Brute Force which will install the brute force agent on the phone, once this is installed keep the device powered*
- Data Extraction Phase in which the device will produce an iTunes backup and will decrypt the keychain. This phase will take approximately 1 hour for every 16 GB of data. The encrypted data will have SHA hash that can be compared to verify that the data was transferred to the forensic machine correctly.

The ability of GrayKey to access a phone depends on the encryption technology resident on the iPhone device. The encryption technology found within iOS 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.

* - depending on the request being made by the submitting agency, the GrayKey technique may stop at the employment of the Brute Force agent onto the iPhone device.

B. Responsibility:

Forensic Examiners

C. Definitions/Abbreviations:

- SEP – Secure Enclave
- SE – Secure Element
- BFU – Before First Unlock
- AFU – After First Unlock

D. Procedure:

The will be two different type of requests associated with the GrayKey software. The requests will depend on whether the submitting agency is requesting that DSS put the brute force agent on the device and return back to them versus if a cell phone extraction will be needed afterwards.

<u>Unlock Agent with Return Request</u>

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 placed in “Airplane” mode.

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

2. Using the lightning cable from the GrayKey hardware, plug in the device and begin the installation process of the brute force agent. Under this type of request, the extraction of the data is not checked off.

3. Once the agent is installed and the brute force process is initiated, the device can be unplugged and then connected to a charging device.

4. The phone can then be placed bag in a secure package and returned to the submitting agency.

5. The evidence will be accompanied with a memo indicating that the Agent has been installed and that the device must continue to be powered. The device will indicate on its screen when the passcode has been determined and that the agency can then uninstall the GrayKey agent. No report is issued in this type of circumstance.

Unlock with Analysis Request

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 placed in “Airplane” mode.

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

2. Using the lightning cable from the GrayKey hardware, plug in the device and begin the installation process of the brute force agent. Under this type of request, the extraction of the data is will be checked off.

3. Once the agent is installed and the brute force process is initiated, the device can be unplugged and then connected to a charging device.

4. The device will indicate on its screen when the passcode has been determined and that the agency can then uninstall the GrayKey agent. The examiner will then record the passcode on QR-CC-57 and will proceed to review the extracted information.

5. Once the data has been extracted, proceed as indicated in CC-SOP-18 (Cell Phone Analysis Protocol). Steps 5 and 6 of CC-SOP-18 will not be applicable since the device will have its passcode determined by the GrayKey software.

6. This request type will have a report generated indicating the results of the analysis.

7. In the event that the GrayKey agent has not unlocked the device after 10 business days after the installation of the agent, the evidence will be returned to the submitting agency.

   Prior to unplugging it, the submitting agency will be contacted and arrangements will be made for the device to be retrieved. The arrangements will include instruction on keeping the device powered so that the brute force attempts can continue running on the device.

   A report will be generated indicated that the agent was installed and that as long as the device is powered, the agent will continue running the passcode attempts.