Smartphone-based Audio Recorder Draft Technical Requirements

Engineering Research Facility, Quantico, VA

29 July, 2016

Smartphone-based Audio Recorder Technical Requirements

1. Background

This document describes the technical requirements for covert, evidentiary audio collection from smartphones. The term "Smartphone" refers to cellular phones that have the hardware and an operating system that are able to run apps to record audio using the built-in microphone, store that data locally, and stream that audio over a data connection in near real-time. This app will allow the phone to be placed into a stealth mode, either by the user of the phone, or remotely by the controller of the phone. In this mode, the room audio will be streamed to another device for live/post monitoring. The basic capability will be audio, but GPS location information is also desired and eventually video capability. This app will run on an Android, iOS, or Windows environment. The phone will operate normally. It will be possible to install the app without having to "jailbreak" the phone. Thus, the app turns the phone into a covert recorder to surreptitiously capture audio and video while also allowing live monitoring.

In addition to the above, the app will also allow the phone to be used *overtly* as an audio/video recorder for capturing interviews. Thus, the Agent can use the phone as a field audio/video recorder when access to standard interview rooms and equipment is not feasible.

2. CONOP

The CONOP involves two scenarios. The first is covert live audio collection from a configured cellular phone. The second is an overt collection of audio and video during an interview (i.e. simply use the phone as a recorder).

For scenario number one, the app would be preloaded onto the phone and run covertly in the background. When the app is running, a person controlling the scenario will be able to remotely enable recording, effectively turning the phone into a local microphone/recorder. The recording will be stored on the phone and simultaneously the live audio will be sent (via the cellular network) to a Government owned server located in Quantico, Virginia. The storage and transfer of data will happen automatically with no user action required.

For scenario number two, the app would be preloaded onto the phone. The person carrying the phone would launch the app and overtly record audio and video for a consensual, one-on-one interview. The video feed of the interviewee will be presented to the interviewer on the screen. The recording will be made on the phone. After the recording(s) has been made, the user will initiate an upload of the files (via the cellular

network) to a Government-owned server. That process will happen automatically with no need for the agent/user to configure network settings.

General principle: any electronic data intended to be admitted in court as evidence will have a traceable "chain of custody" and procedures to ensure it has not been altered or tampered with. This app shall contain technical safeguards designed to protect the stored evidence. While authentication hash is required, encryption is not necessary, as the recorders do not store classified information.

3. Basic Requirements

This section lists the minimum technical requirements for meeting the two concepts of operation. The main deliverable for this effort is the app which shall be compatible with Android, iOS, and Windows platforms, and the server-side software necessary for receiving the data. The app shall have two main functions: live monitor and interview recorder. Upon loading the app, the user shall have the option of selecting between these two modes. Each Concept of Operation (ConOp) will be covered in its own section.

3.1. ConOp #1 (Live Monitoring) Application Requirements

Following are specific technical requirements pertaining to use of the Smartphone for covert, live monitoring.

3.1.1 Live Monitor

The live monitor ConOp shall have three roles: one is the phone that sends out the data (the recorder), one is a phone that can receive the data and listen in (a listener), and one is a phone that can remotely control the sending phone (a controller).

3.1.1.1 The controller shall have control over the operation. The controller shall be able to turn the audio and GPS location transmissions on and off.

3.1.1.2 The recorder shall also have the capability to turn the audio and GPS location transmissions on and off.

3.1.1.3 Any listener shall only have the capability of monitoring the audio and/or GPS transmission when enabled.

3.1.1.4. The controller shall have the ability to set the phone to send audio, video, and/or GPS data without storing it on the phone or server. This is intended for an

"officer safety" scenario, and to allow for live minimization when required by court order.

3.1.2 Operation Start Up

3.1.2.1 The live monitor app shall open when selected by the user.

3.1.2.2 Every user shall be prompted to enter a pre-arranged authorization code, before the operation can start. This operation code(s) shall be predetermined by the vendor and shall be unique for each new operation.

3.1.2.3 The unique code shall be required for any other phone to join the operation. Once entered, the code is confirmed with the controller unit for user authorization.

3.1.2.4 Once a user has been granted access to an operation, that user shall be required to select a recorder or listener role.

3.1.2.5 Only one recorder shall be permitted per operation.

3.1.3 Monitoring

3.1.3.1 The app shall stream the audio over the cellular network to a Bureau controlled server.

3.1.3.2 Any user shall be able to listen to the audio and monitor the target location via GPS to a displayed map. (The displayed map can be Google Maps.)

3.1.4 Recording Requirements

The app shall record the audio on the target phone ("recorder") and also stream the audio to a Government server with a public-facing IP address.

3.1.4.1 The audio streaming shall be accomplished via the cellular network.

3.1.4.2 The audio shall be saved on the recorder in an uncompressed or lossless manner.

3.1.4.3 The audio files shall be stored in standard WAV format.

3.1.4.4 The recorder shall sample audio at 16 bits.

3.1.4.5 All files shall be date and time stamped.

3.1.4.6 There shall be no way to edit recordings on the phone.

3.1.4.7 Once the on board memory is full, recording shall stop so there is no loss of already-recorded data.

3.1.4.8 If the memory is full, streaming of audio shall continue if network coverage is available.

3.1.4.9 If the memory is full, an alert shall be sent to all other devices in the operation that the memory is full.

3.1.4.10 The app shall implement a cryptographic hash function such that all recorded data can be authenticated. Calculation of the hash shall be performed on the phone. This calculation can be done at the time of recording, the time the file is closed out, or at the time the transfer to the server is initiated, at the vendor's discretion, to minimize battery drain.

3.1.4.11 The hash algorithm shall be SHA-1 or SHA-256. Reference:

- Secure Hash Standard, FIPS Publication 180-4, dated 6 March 2012, available at: http://www.nist.gov/manuscript-publication-search.cfm?pubid=910977

3.1.4.12 The hash message shall be saved in an associated XML metadata file that will be uploaded along with the recordings.

3.1.4.13 The vendor shall implement a data transfer method that ensures that the data on the recorder exactly matches, bit for bit, the data transferred into the server.

3.1.4.14 The recorder phone shall not erase the data after it is transferred without a separate, deliberately initiated, on the part of the user.

3.1.5 Graphic User Interface

3.1.5.1 The software shall emphasize simplicity and ease of use.

3.1.5.2 Controls which are administrative or seldom used shall be hidden from the main user screen.

3.1.5.3 The main screen on the controller, shall at a minimum, have a map showing the transmitter location and whether data is being received.

3.1.5.4 The map shall be scalable by user using two fingers on the touch screen.

3.1.5.5 While in live audio mode, the phone being used as a covert recorder shall have a means to hide the fact that it is recording and streaming audio. The vendor can implement this as a fake app, or a hidden app that requires a special input (like a pattern of taps or swipes) to bring it into view, or some other method, at its discretion.

3.2 ConOp #2 (Interview Recorder) Application Requirements

Following are specific technical requirements pertaining to use of the Smartphone for overt recording of interviews by a law enforcement official.

3.2.1 Interview Recorder - The interview recorder ConOp shall have a single user designation: interviewer.

3.2.1.1 The user shall have the capability to start and stop the recording.

3.2.1.1.1 The app shall give an audible indication when recording has begun and stopped.

3.2.1.2 The user shall have the capability to end the session, thereby prohibiting any further recording on that session.

3.2.1.3 The user shall have the ability to play back the interview.

3.2.1.4 Upon start up, the app shall offer an interview function.

3.2.1.5 The user shall be prompted to enter a case number.

3.2.1.6 Start, pause and stop buttons shall be displayed after a case number is entered.

3.2.1.7 The recorder shall record audio at 16 bits or resolution (unless the phone hardware does not support this, then use the highest possible resolution).

3.2.1.8 Video shall be stored and uploaded using Motion JPEG (MJPEG) and/or H.264/MPEG4 AVC (assuming the phone supports this).

3.2.1.9 Video recording frame rate will be determined by the hardware available on the phone. 30 frames per second is preferred. The app should support the best possible quality available from the phone.

3.2.1.10 The video should be saved at resolutions of 640x480 ("VGA") at minimum. Note that high resolution is not necessary, and wastes bandwidth and battery life.

3.2.1.11 The video picture shall appear on the phone.

3.2.1.12 The video shall have time, date and case number superimposed on the video.

3.2.1.13 The video and audio streams/files shall remain synchronized to an accuracy of 33 msec throughout the duration of the recording.

3.2.1.14 The clock shall count in real time.

3.2.1.15 The software shall emphasize simplicity and ease of use.

3.2.1.16 Controls which are administrative or seldom used shall be hidden from the main user screen.

3.2.1.17 For playback the main screen, shall at a minimum, display the video with play and stop buttons.

3.2.1.18 It shall be possible, using a slide line, to skip video to any part of the recording for quick review.

3.2.1.19 The app shall implement a cryptographic hash function such that all recorded data can be authenticated. Calculation of the hash shall be performed on the phone. This calculation can be done at the time of recording, the time the file is closed out, or at the time the transfer to the server is initiated, at the vendor's discretion.

3.2.1.20 The hash algorithm shall be SHA-1 or SHA-256. Reference:

- Secure Hash Standard, FIPS Publication 180-4, dated 6 March 2012, available at: http://www.nist.gov/manuscript-publication-search.cfm?pubid=910977

3.3 Server-side Requirements

The phone and its app is only half the system. The other half is a web-facing server that will reside in a secure, Government-owned space. Note that at that point, the data officially becomes "evidence," therefore, many of the following requirements pertain to the specific file format and metadata that the files must have. It is likely that the Government will want to obtain server software from the vendor, and will install and maintain that server after the software has gone through testing and a security accreditation process.

3.3.1 Operational Metadata

3.3.1.1. The server will run software that allows for a super controller (which is different from the server admin) to manage the operational codes (ref 3.1.1. above).

3.3.1.2. At the time an operation is set up, the controller will have the ability to request an operational code. He will be required at that time to enter case-related metadata that the server will associate with the operational code.

3.3.1.3. The user of the recorder phone shall be asked to input certain information that will be transmitted along with the audio files as metadata. This will be processed by the server prior to issuing an operational code. The specific information will be provided to the vendor as GFI (Government Furnished Information), but will be similar to this:

- Field Office: enter the field office location
- Case Number: enter up to 8 alphanumeric characters
- Property Number: enter an 8 alphanumeric inventory control number
- Comments: freeform text for user notes (optional input)

3.3.1.4 The system shall provide appropriate metadata in a specified XML schema. (Note the specific fields used in the Schema will probably change over time, but will be formally specified and provided to the vendor as GFI.)

3.3.2 File Delivery

3.3.2.1. The server software shall package and deliver the recordings and recording metadata inside a ZIP container. Each ZIP container will correspond to a single recording. We will work with the vendor to determine whether long recording sessions should be broken into smaller files (due, for example, to cellular network limitations) and how these would be aggregated into a single container.

3.3.2.2. The server will use SFTP (Secure File Transfer Protocol) to transfer the ZIP containers to a "watch folder" on another server on a Government network.

3.3.2.3 The server shall name each ZIP container with a specific format to be provided as GFI.

3.3.2.4 Each media file, GPS log file, and metadata file within the ZIP container shall have a file name that conforms to a specific format to be provided as GFI.

3.3.2.5 Each individual recording made on the phone and its metadata shall be placed in its own ZIP container. Thus, each ZIP container shall contain exactly the following four files: the media file (.WAV, .AVI, etc.), the related metadata file (.XML), the GPS data file (.CSV, .KML, etc.) and a text file with the SHA hash message.

3.3.2.6 The ZIP container shall be packaged using a method that can be extracted by pkzip (which is incorporated in Windows 7 and later). It shall not be compressed, however. ZIP is merely being used as a commercial standard container.

3.4 Manual transfer of files off phone

3.4.1. Automated transfers of data from the phone to the server are preferred. However, there are situations in which this might not be possible for some reason. In those cases, there shall be a method for a trained, authorized user to transfer recordings directly off the phone.

3.4.2. The preferred method is via simple USB connection of the phone to a PC, which is mounted, and normal Windows file explorer operations. The user will need to know where the app stores the files.

3.4.3. The files will be encrypted, with the password (key) the same as the operational code.

3.5 Support

3.5.1 Software Modifications

3.5.1.1 The vendor shall update the app for each platform (e.g. Android, iOS) as needed, to ensure compatibility and functionality is maintained as the operating systems change and evolve.

3.5.1.2 The phone app updates shall be implemented yearly, at a minimum.

3.5.1.3 The vendor shall have a procedure to perform the app update without need of "jailbreaking" the phone. An example of how to do this is to make the app available for download via an app store (examples: iTunes store, Google Play Store).

3.5.2 Training

3.5.2.1 The Contractor shall provide in-depth training to as many as 10 Government technical personnel covering operation and testing of the software. The primary goal of the training is to enable the 10 to provide detailed support to many end users. They must be able to troubleshoot problems and have intimate knowledge of the design of the software.

3.5.2.2 This training will be in the form of a briefing and informal, hands-on demonstrations that can be performed at the Contractor's location.

3.5.2.3 Any documents used in the training shall be provided as a deliverable to the COR.

3.5.2.4 The vendor shall also prepare video tutorials describing all features of the software for both users and administrators.

3.5.3 Legal support

3.5.3.1 On occasion, the authenticity of an evidentiary recording is questioned in court, and someone must be put on the stand to answer detailed technical questions about the audio/video collection. Responses to this scenario are provided by trained Government personnel whenever possible. Typically the response is for the vendor to sign an affidavit that addresses the specific question raised, and only that question. There is a remote possibility that an affidavit is insufficient and a vendor representative could be subpoenaed to appear in person to provide court testimony. Generally this involves giving a technical or scientific explanation of the collection technique with the goal of establishing or ruling out the possibility of tampering. Any vendor-proprietary information can be protected with limited dissemination, proprietary markings, and need to know. In fact, the Government works diligently to limit and control who has access to these details as they could be used against us. Historically these scenarios occur no more than 3 times per year. The vendor must agree to this possibility and provide a point of contact (must be a US Citizen) who can support such a request.

3.5.3.2 The vendor will be asked to support a security accreditation process on the server. This means the code on both the phone app and the server will be examined, and the system behavior tested, by Government personnel. The purpose is to prove that data transfers go only from the phone to the server and only from the server to the specified network IP address, and to no other location or IP address. The support required from the vendor for this accreditation process could be as minimal as answering questions, to at most submit source code, explain its operation, and correct deficiencies that may be discovered. It is assumed this might involve proprietary information and non disclosure agreements.

3.5.4 Warranties and Maintenance

3.5.4.1. The vendor should describe the warranty terms available for this product.

3.5.4.2. The Contractor shall make available a list of technical points of contact that can be called or e-mailed during normal business hours (approximately 8AM-5PM) by Government personnel.