Specification of Bodyworn Cameras

1. Video

1.1 Recording

1.1.1 It should be possible to start recording by pressing a single button

1.1.2 There should be a positive action on/off button, so that the user can feel whether they have successfully switched the recorder on or off.

1.1.3 Stopping recording should require a minimum of two actions (eg. Pressing two buttons), to reduce the possibility of accidental shutdown.

1.1.4 A clearly visible indicator (s) should denote when the device is on and actively recording.

1.1.5. The field of view to be covered by the lens should approximate the human visual system, ie, about a 40^0 horizontal angle of view.

1.1.6 The camera(s) must have a focal length such that an object 1.8 m (5'9") tall will fill 50 % of the viewing height at a distance of 7 m.

1.1.7. Recording must be in a non-proprietary, standard file format to enable replay on domestic DVD players and computers (PSs and Macs) without conversion.

1.1.8. The recording device should not permit the editing or deletion of recordings. The data will be deleted only after it has been archived to a computer, at which point the hard disk drive (HDD) or other storage medium will be wiped clean. However, the procedure to wipe the drive will be controlled from the archive computer to which the storage medium is connected, and not the recording unit itself.

1.1.9. Each recorder should have a unique serial number.

1.2 Image quality

1.2.1 Recording should be at 25 frames per second

1.2.2. Recording should be at a minimum of VGA (640X480) resolution.

1.2.3. The quality of the recording should be such that an individual should be

recognizable up to a distance of 7m from the camera.

1.3. Storage

1.3.1. The recording device must be able to store a minimum of 24 hours of video for a hard-disk based recorder. For a Flash card based system, the recording capacity should be more than the expected battery life.

1.3.2 Filling the recording device should cause the device to cease recording - existing data must not be overwritten.

1.3.3. Data should be filed in a Windows-readable directory structure.

1.3.4. Incidents should be stored in separate directories (An incident is defined as the period between the start and stop buttons being pressed)

1.3.5. Long recording should be split into segments, each of which is a maximum of 2 GB in size. These files should be stored in the same directory and must be playable as one continuous piece of footage.

1.3.6. File names should comprise the serial number of the unit and the date and time of the recording.

1.3.7. Metadata (comprising unit serial number, date and time) must be displayed on the screen in a legible but unobtrusive manner)

1.3.8 Data must be stored on a removable medium (eg removable HDD, Flash memory card etc) and/or it should be possible to down load the data from the recorder via a cabled download mechanism of a suitable speed, such as USB 20. Or Fire wire (400 or 800). The download rate must be no lower than 350 MB per second. USB 1.0 is not suitable for this purpose as the download rate is inadequate.

1.4. Playback

1.4.1 The recording device should provide a replay facility via an inbuilt screen.

1.4.2. The display screen on the recording device will be high resolution to clearly display the metadata overlay on the image.

1.4.3. The device should be capable of searching the incidents recorded by date and time to find the incident of interest. Once this recording has been loaded into the replay window, it should be possible to wind through it to identity the specific event of interest by means of fast forward, rewind, play, pause and stop controls or with a scroll-bar

mechanism.

1.4.4. Where a long recoding has been split into separate files, the playback mechanism should retrieve the complete recording and allow seamless replay of the entire incident.

1.4.5 A live view display option should be available, to assist the officer to set the camera position and provide confirmation that the system is connected correctly.

1.5. Audio

1.5.1. Audio should be stored in a non-proprietary format, replayable on domestic DVD players and computers.

1.5.2. Audio should be synchronised with the video recording.

2. Physical

2.1 The mounting for the camera will not move after being set by the officer.

2.2. The recorder must have the means to be securely attachable to a police officer's belt.

2.3. The microphone will be positioned along the cable connecting the camera to the recorder, in order to capture both the officer's speech and that of the other parties to the conversation.

2.4. Cable connections from the camera and microphone to the recording device will have a break point as safety feature to reduce the risk of injury to the officer. This should be located after the microphone but before the camera in the recording chain. Te cable should be coiled to reduce the amount of exposed cable and so that it moves easily with the officer's head.

2.5. Capture, record and storage device(s) should be sufficiently robust to withstand daily use in an operations police environment for eg. the recorder should have physical protection against knocks, should be shock and vibration -proof and should be able to record while the officer in running.

2.6. Interface controls must be of sufficient size and easily used by an officer

2.7. The unit must have a maximum total weight of 500 gm.

For body-mounted cameras

2.8 Body mounted cameras should face forward and capture the scene that the officer has their body facing towards.

3. Environment

3.1 Ingress protection of camera (ie protection from dust and water) to IP 6521 standard.

3.2. The temperature range of operation should be up to $+50^0$ C

3.3 The system should not interfere with other electronic equipment carried by the officer, particularly by the wireless system.

4. Battery

4.1 Rechargeable batteries are essential

4.2 A fully charged battery should provide power for at least eight hours' continual recording.

4.3 Batteries should be removed from the recording unit to be recharged, so that the recorder does not have to be withdrawn from service while recharging occurs.

5. **Troubleshooting**

5.1 Suppliers of the system should provide an adequate support network in the event of equipment failure.

Desirable Features and Considerations.

6. Additional features

6.1 Check sum of each file as it is created.

6.2 An audit trail in the device should be able to monitor usage, activation, reply and copying of footage from the device and further down the evidential chain to prevent unauthorized release of video or arguments over system deployments. This should be separate from the image file and completely un alterable. It should be in an easily readable form that a layperson can understand.

6.3 A function to allow recording and simultaneous reply of material would be desirable.

6.4 A Camera with a rating of IP 67

6.5 Upgrading firmware/ software should be straight forward and should not require any connection to the internet.

6.6. There should be time synchronization capabilities that an administrator can perform to ensure the units are all locked to exactly the same date and time.

6.7 Measures should be taken to prevent accidental unit shutdowns.

6.8 Screensavers would be desirable to save on battery life.

6.9 A targeting device on the camera is desirable to enable accurate recording for the Officer. This should raise no safety issues and it should not be possible to activate this accidentally.

6.10 Devices/recording media should be tied to a particular workgroup of computers (as with multimedia players such as iPodes) to prevent accidental download of material on to an unsecured computer, but there must be a facility for administrator override.

6.11 The supplier should data recovery assistance in the event of a catastrophic system failure.

6.12 An audible alarm should sound when the device is 95% full.

6.13 Metadata could be displayed onscreen in a user defined position.

6.14 A global positioning system (GPS) could be integrated in to the device that activates when the system is recording to document officer movement within an incident; this would be to show, at minimum , officer location(longitude and latitude), heading and altitude.

6.15 A barcode system of checking units in and out from the storage facility

Archive And Retrieval System

System Over view

This sets out the specification for the back office facility for the storage, reply and archiving of video taken from BWV devices. The solution will ideally be computer (PC) based and should allow the user to:

- Download video from the body-worn camera;
- Review video on the system;
- Create master and working copies of evidential
- Material on WORM media; and store non-evidential material for 31 days before deletion.

Mandatory Requirements.

1. **Hardware**

1.1 The minimum amount of storage space is 1TB, although upgradable storage is desirable.

1.2 A RAID I redundant drive for hard drive failure should be incorporated, with alarm functionality to notify failure. Operation should continue unaffected using the remaining hard drive.

1.3 Master and working copies to be created on WORM media. WORM facility must consist of at least two drives to create a master and working copy simultaneously, although more drives may be required depending on police force requirements. Given the large volume of data to be archived, DVD drives (as a minimum) would be appropriate.

1.4 connection to the BWV systems must be present, ie, USB 2.0 devices, Flash card reader, Firewireport, caddy for removable hard drive etc.

2. Software

2.1 The graphical user interface should be a simple wrapper to allow a user to perform only the following functions:

2.1.1 Log in to system.

2.1.2 Download new video to the system from the recorder.

2.1.3 Add label of Officer ID (and the ID of person entering data onto system if different)

2.1.4. Software should prompt the officer to decide whether the footage is evidential or non-evidential.

2.1.5.Search data on the system by date and time of recording, recorder serial number, Officer ID and whether data is evidential or non evidential

2.1.6. Review data using simple play, fast –forward and rewind buttons.

2.1.7. Frame –grabbing function to save stills from the file, and the ability to print out these images.

2.1.8. Allow Officer to change status of the footage from non-evidential to evidential or vice-versa.

2.1.9. Create a master and a working copy by clicking one button.

2.1.10. User access must be limited to the graphical user interface and prevent access to the desktop.

2.1.11 Officer incident logs must be added to the system and filed alongside the video data, either by scanning in a handwritten document or by means of computer generated forms.

2.2 Administrator function (password) protected to allow access to the desktop, install upgrades to firmware and software and to view and print the audit log.

2.3 The decision as to the status of the evidence must be made at the point of data input. The software will then tag evidential and non-evidential material differently. Non-evidential data should be auto-deleted after 31 days. Evidential forage should be deleted after the creation of the mater and working copies (and verification.)

2.4. The verification process must occur after the footage has been downloaded (from BWV) to computer, and then from computer to WORM) to ensure that all data has been accurately transferred.

2.5 When it has been confirmed that the video has been transferred successfully from the BWV to the back office system, the data should be wiped from the BWV so that unit can be redeployed.

2.6 There must be no facility for editing filed.

3 Audit trail

3.1 The audit trail must contain the following items, with dates times and user details of their creations and amendments:

- When data is added to the archive system;
- When data is reviewed;
- When the status is amended;
- Who has viewed the file;
- When the master is created;
- When a working copy is created; or
- When the data is deleted.

4. Disk management

4.1 The system should not over- write existing material that is wither:

- Non evidential and less than 31 days old; or
- Evidential and not archived to WORM

4.2 The warning message must occur when the HDD files to 95% of its capacity. If the HDD is full, then the system should stop accepting new data.

4.3 A warning message should appear on log-in if evidential data has not been archived, detailing those files that need to be archived.

5. Troubles shooting

5.1 Suppliers of the system should provide an adequate support network in the event of equipment failure.

Desirable features and considerations:

6. Additional features

6.1 Frame advance and rewind so that video can be closely scrutinised.

6.2 The supplier should provide data recovery assistance in event of a catastrophic system failure.

6.3 Automated writer, stacker and label printer for master and working copy creation.

Also Provide 3 docking stations with minimum capacity of 5 BWCs capable of automatically uploading content on to a PC in addition to charging the BWCs.

Warranty – 3 Years

AMC - 3 years after warranty period