Strategic Policing and Crime Board

16 October 2018

Police and Crime Plan Priority: *Building Trust and Confidence in Our Police*

Title: *Mobile Fingerprint Identification*

Presented by: *Ch. Supt. Steve Graham/Nigel Johnston/Alison Fernyhough*

PURPOSE OF REPORT

1. The purpose of this report is to provide information regarding the purchase, deployment, training and use of the replacement Mobile Identification Devices that will be issued as part of the Smarter Responding Project. This paper is for discussion.

REQUIREMENTS

2. Until 31st March 2018, the force had a number of 'Lantern' devices that previously offered the mobile identification solution for the force. These devices were withdrawn as the contract with the provider ceased at the end of March 2018 due to the Home Office no longer supporting the product. At the time of the contract ending, the force had 30 Lantern devices with 24 of them in operational use.

3. The loss of the previously used 'Lantern' devices revealed a capability gap in that officers were unable to prove a person's identification whilst mobile.

4. Currently, in circumstances where officers are unable to confirm a person's identity, they are required to transport them to a custody suite where their identity can be confirmed using Livescan, the dedicated fingerprint identification system used within custody suites. This process is inefficient due to the time spent escorting suspects for the sole purpose of identification. Officers are also removed from public view and unavailable to repond to incidents at pace.

5. This also places additional demand within custody environments which causes unnecessary delays to other on-going investigations. If an officer can identify a nominal without the need to visit a custody suite, the demand for custody space and time for this type of enquiry reduces considerably and increases officer efficiency.

6. A wider roll-out of Mobile ID capability supports the ambition to be truly mobile, equipping officers with real-time intelligence and the ability to respond at pace.

7. A market and technology review examining future opportunities was completed by the Project Team to support a 'value for money' assessment prior to the wider roll-out of Mobile ID. The selected device, the Watson Mini, works by plugging into the current mobility devices. Following the roll out of the first 100 devices, data will be collected detailing usage ahead of procurement and roll out of further devices to ensure maximum benefits are realised. The external devices will need to be procured by West Midlands Police and can be extended to all officers.

8. The technology behind the device forms part of the Home Office Biometrics (HOB) Programme and will provide a single universal access point to the current biometric systems – referred to as a "common front door" from which new capabilities can be delivered and services consolidated. The Biometric Services Gateway (BSG) has been created to provide this "front door" capability.

9. The BSG replaces the end-of-life infrastructure that supports a critical part of the communications between Home Office systems, with a single modern platform. Additionally, the upgrading and rationalisation of interfaces enables increased transaction volumes between HOB systems. Beyond the immediate benefits, the BSG provides the back bone of the HOB Programme supporting future transitions and improvements.

10. HOB ensure compliance between WMP and the BSG Code of Connection.

CAPABILITIES & BENEFITS OF MOBILE ID

11. Mobile ID will rely upon an external fingerprint capture device, whether it be wired or wireless. If identity is in doubt the officer simply requests the subject to place their finger onto the plugged in device. Information, including a PNC check, will then be available for review on the officer's mobility device. The solution will extract the captured prints and then process them for submission to IDENT1. IDENT1 is the single, searchable database for the UK mainland for finger and palm print data. Fingerprints are currently the only viable biometric for 'real time' identification against a UK National database currently of around 9 million records.

12. There are number of identified benefits of Mobile ID including, but not limited to:

- A reduction in the number of arrests in order to confirm identity

- Obtaining real-time data and intelligence to support identification whilst mobile

- Reduction in time spent travelling to custody suites

- Can be utilised to identified victims in suspicious deaths, road collisions and incidents such as drowning

- Provide reassurance to our communities that the criminal justice system will not be frustrated by individuals who provide false information

STATUTORY BASIS OF THE USE OF MOBILE ID

13. Officers can use Mobile ID in the course of their duties if there are reasonable grounds to do so, covered under the General Police Powers. This can arise during Stop and Search, Section 163 Road Traffic Stops and Section 60. A fingerprint is taken with consent and if refused, officers can revert to their usual powers of arrest in order to confirm a person's identity.

14. Should the officers get a hit on the device from the immigration database the officers would take the individual into custody where UK Border Force would be contacted to deal with them in line with current operating procedures.

15. Below are two scenarios that demonstrate best practice with the use of Mobile ID:

SCENARIO 1:

16. The Mobile ID device helps identify a suspect wanted for serious crimes with a vulnerable victim. The identification was made after Police Officer's stopped a vehicle suspected of having no current insurance or known keeper. A Mobile ID device was used and his real identity was quickly established. The man was wanted for a number of fraud offences in another Police Force's territory. The victim an 85 year old female has been subject to a £25000 fraud and had been wanted for a number of months. His arrest supported a vulnerable victim and the associated police time in trying to locate the suspect.

SCENARIO 2:

17. The Mobile ID device helps identify wanted suspects. A vehicle was stopped by officers following reports for routine traffic offences. The occupants were all foreign nationals, spoke little English and produced a number of identification documents. A Mobile ID device was used on the two occupants however their fingerprints did not match those of the details they had provided, as their fingerprints were linked to other nominals. The officer's suspicion were raised and he was then able to establish these persons were in fact two Syrians wanted for a number of offences including their deportation from the UK.

DATA HANDLING

18. Data is held using the same regulations as Livescan, PNC and IDENT1.

LEGITIMACY

19. The Mobile ID device can not be used without the consent of the person involved in the check. Officers are unable to use the device without having a just reason under their General Police Powers or reasonable grounds to suspect a criminal offence has been committed. All transactions will be audited through Hendon with audit reports produced monthly to the PNC Bureau and Professional Standards. Any unusual activity will be

highlighted on these reports. Unusual activity will then be investigated by the appropriate departments.

OFFICER TRAINING

20. Officers require no formal training in the use of Mobile ID as the device works in the same way as the previous 'Lantern' devices. A user guide with general points has been written and will be available on the intranet, including the consequences of misuse as per exisiting procedures. Officers are aware of their powers of use which forms part of the Student Officer Training. Force-wide communications announcing the new devices has already taken place. Further communication is planned during the 'go live' phase.

OPERATIONAL AND MANAGERIAL MECHANISMS AGAINST MISUSE

21. Regular audit reports will be produced on the activity of devices. The reports will be produced from the PNC and Mobile ID Audit dashboard. The reports will be run every month and reported to Information Management and Professional Standards.

FINANCIAL IMPLICATIONS FOR FURTHER ROLL OUT

22. A pooled roll out of up to c650 devices has been supported by the organisation with an initial 100 devices procured for users across the force to understand usage and benefits prior to wider implementation. Each device costs £395.89 with the total costs and volumes outlined in the table below. Costs for further accessing the Biometrics Gateway Service are yet to be confirmed.

User Segment	Pool Issue (20%)	Cost (£400 per device)
Force Response	233	£93,280
Operations	152	£60,640
NPUs	272	£108,960
Totals	**657**	**£262,880**

NEXT STEPS

23. The board is asked to note the report and the Project Team will be available to answer any relevant questions.

Author(s): Alison Fernyhough

Job Title: Project Manager – Smarter Responding