Justice Sub-Committee on Policing

Police Scotland's digital, data and ICT strategy

Police Scotland's Proposed Use of Digital Device Triage Systems

This letter is for the attention of members of the Justice Sub-Committee on Policing, and provides a written response to points that were raised in your letter dated 15 May 2018. It is also hoped this response will help inform the Committee Evidence Session on the 21 June 2018.

Financial Investment & Procurement

In relation to costs associated with the procurement and on-going management of the 41 cyber kiosks the following information can be provided.

The Cyber Kiosks procurement was performed in compliance with The Public Contracts (Scotland) Regulations 2015 and the Police and Fire Reform (Scotland) Act 2012. The Terms and Conditions of the Crown Commercial Service Technology Products 2 Framework RM3733 applied to the purchase of this solution. Funds were allocated from the Capital Transformation Funding 2017/18.

- £444,821 Inc. VAT – This is the up-front cost related to the purchase of the Cellebrite Kiosks, the central management software used on the devices and training package.

- £101,000 – This relates to the annual revenue support cost which will commence from 2019/20.

You specifically requested an explanation of the following published costs:-

a. £431,000 – Abbott Informatics
b. £286,571 – eDiscovery and Analytics Software
c. £445,000 – Cellebrite kiosks, licences and training package
d. £100,000 – Cellebrite annual fee

The items noted above for a. Abbott Informatics, b. the eDiscovery and Analytics Software and c. Cellebrite Kiosks, licences and training package were published on the Scottish Government's procurement portal Public Contract Scotland on 5th and 6th April 2018. As mentioned item d. Cellebrite annual fee is the recurring revenue support cost for the Cellebrite Kiosks. To further clarify, Abbot Informatics is procurement for SPA Forensic Services and is a tool to extract performance management information from the current SPA Forensics Examination Management System (EMS). It is not related to Cyber Kiosks. The eDiscovery and Analytics Software procurement is to support enhanced analytical & capability within Police Scotland's Digital Forensics Hubs and is a distinct and different capability than that provided through Cyber Kiosks. The items referring to Cellebrite are in relation to the Kiosk procurement and initial revenue cost. Exact details of costing are as detailed. The Cyber Kiosks are a standalone technology.

As you are aware Police Scotland has been in the process of developing its Digital, Data and ICT Strategy. Briefings with the developers of this strategy occurred to ensure that the proposed on-going transformation of the Digital Forensics Hubs, including the introduction of cyber kiosks, was not contrary to the considered direction of the strategy.

Policing 2026 is the most significant period of transformation and modernisation undertaken by policing in Scotland. The Digital Forensic Infrastructure project was established to build a consistent framework of digital forensic services within Police Scotland. Cyber Kiosks were identified as a key deliverable in supporting the aspiration to digitally enable frontline officers and provide greater access and improved delivery of cyber digital forensic capabilities. As a consequence the procurement of cyber kiosks was included in the 3 year implementation plan as a way of maximising efficiency, improve service delivery and thus provide capacity to modernise.

The technology behind Cyber Kiosks has been available to United Kingdom Law Enforcement since the late 1990's and the software is routinely used by Police Scotland Cybercrime Digital Forensic Teams within the existing Hubs. While the technology is not new to Police Scotland, the proposal to make some of the capability available to suitably trained frontline officers, in a triage format, forms a key deliverable within the digital strategy aimed at driving efficiency and improving service delivery.

Trials

The trials undertaken in 2016 in Edinburgh and Stirling were to consider those devices which had been legally taken by frontline officers and which would necessitate a submission to Cyber Digital Forensics for full examination. The trial was to consider the viability of introducing a triage system, the advantages to frontline officers and the public, the benefits derived from reduced submissions to Cyber Digital Forensics as well as any additional training implications for those concerned. Subject to the outcomes of the trials, it was already accepted there would be wider implications for data privacy & security and that current protocols would require to be reviewed. This activity was agreed by Senior Managers within Cybercrime in consultation with managers within Local Policing and external consultation with COPFS.

Over the trial period a total of 195 mobile phones and 262 SIM cards were examined using the terminals in Edinburgh and in Stirling 180 mobile devices were examined. Again, it is worth noting these items had all been legally taken as part of a police investigation and would have been submitted to Cyber Digital Forensics for full examination.

A cadre of officers were identified in both areas and trained in the use of the technology and provided input on the policy for digital device seizure and associated legal basis. Trained users had the ability to conduct a triage examination of a lawfully seized device.

To reiterate these technologies already existed within Police Scotland and were in use. There was therefore no policy change; instead an extension of existing capability and it was already accepted there would be wider implications for data privacy & security, that current protocols would require to be reviewed and this would necessitate a wider engagement to inform the required impact assessments. To confirm these assessments are on-going as part of the policy development including consultation process. No assessments i.e. human rights, equalities, community impact assessments and data protection and security assessments were completed prior to trial commencement.

The SPA receive regular updates on policing matters, including cybercrime and although no specific briefing to SPA occurred prior to trial commencement the proposal to procure cyber kiosks was presented and supported at Police Scotland Change Board. In relation to owners of devices which were subject of an examination it should be noted that any device subject of an examination by cyber kiosks requires to be seized for a lawful policing purpose. The owners of those devices, process dictates would be been informed, by the investigating officer(s) that the device was being seized as evidence and would be subject of a forensic examination.

You have requested clarification on a number of points in consideration of the trials. To confirm the data collated at this time was in terms of number of devices examined. Further data in terms of nature of seizure, specific lawful policing purpose under which the device was seized and subsequently examined and the evidential efficacy of those examinations in supporting a prosecution were not collated. The reason for this being that this was not the purpose of the trial. The trial was to test the usability of the technology by front end officers and to better understand the potential to improve efficiency in the service.

Prior to the trial period and during the current procurement and development phase consultation with other United Kingdom Law Enforcement utilising this technology has continued.

You specifically requested two existing reports of the trials. These are attached to this response (Appendix A Memo - Telephone Kiosk Trial; Appendix B Kiosk - Trial Business Case) but are redacted under the terms of the Freedom of Information (Scotland) Act 2002 and pertain to removal of direct email addresses and telephone numbers, investigative matters and matters of commercial interest. It should be noted that in April 2018 both redacted reports were provided to a specific requester in response to a Freedom of Information Request.

These reports provide a narrative of observations made by those involved in the use of the technology and justifications to support a wider programme of delivery e.g. reduced submissions requiring full digital forensic examination, enhanced service to public as many devices returned at much earlier stage and the provision that specialist resource increase time spent in the investigation of serious and complex cases, maximising public protection and accelerating investigations all to the benefit of the public.

Consultation with COPFS

Prior to the commencement of the trials PSOS sought advice from Senior Managers within the Crown Office Procurator Fiscal Service (COPFS). COPFS agreed to the trial in the East of Scotland on the basis that any triage of devices were assessed at the time to be relating to what were expected to be summary cases. PSOS updated the COPFS representatives as the trials progressed. Upon the trials conclusion PSOS updated the COPFS and sought support for the wider roll out of the triage devices to support all types of criminal enquiries. No specific issues were raised by local Prosecutors in relation to the 2016 Pilots. Related correspondence is attached (Appendix C – All Emails Redacted.) Similar to previous Appendices the correspondence is redacted under the terms of the Freedom of Information (Scotland) Act 2002 and redactions pertain to the removal of direct email addresses and telephone numbers, investigative matters and matters of commercial interest.

COPFS representatives attended the most recent Gold Group meeting held by Police Scotland in relation to Cyber Kiosks and will have a representative on the External Reference Group to consider issues arising including consideration of policy documentation to support Cyber Kiosk use.

On-going Assessment and Consultation

To confirm an Equality & Human Rights Impact Assessment (EHRIA) and Data Protection Impact Assessment (DPIA) are on-going. Part of the process for completion is consultation and development and finalisation of the supporting policy, practice and procedures. These assessments will therefore be completed once all consultation is complete and supporting documentation finalised.

On Thursday 24 May 2018 Police Scotland provided a demonstration event in respect of the Cyber Kiosks. Invites were extended to representatives from Scottish Police Authority (SPA), Her Majesty's Inspectorate of Constabulary in Scotland, (HMICS), Crown Office and Procurator Fiscals Service (COPFS), Information Commissioner, Scottish Police Federation, Scottish Government and members of the Justice Sub-Committee on Policing. As well as providing a demonstration of the equipment, this event provided an opportunity to examine how Cyber Kiosks will be used by front-line officers and the policy around data privacy and security.

A reference group is to be established which will shape the delivery and communication strategy as well as having the opportunity to consult on the proposed policy, practice and procedure to support operational delivery of this technology. The outcomes of this consultation and engagement will inform finalised training and roll out timelines. The final membership of this group is still to be established. It is the intention of Police Scotland to ensure the group comprises of organisations and individuals who have raised specific concerns around the wider deployment of this technology.

Prior to finalisation ACC Steve Johnson, Senior Responsible Officer (SRO) for the Cybercrime Capability Programme which includes this project of kiosk deployment will consider and approve the supporting policy, practice and procedure.

Kiosk Functionality

The Kiosk is a desktop personal computer which has a single function – to examine mobile devices using built-in software. Assessments are usually made by viewing the data on the Kiosk's screen. It may be that the amount of data extracted from a device is extremely large, in which case it can be extracted to disc using the Kiosk's built-in disc writer. Police Scotland is currently considering the use of this functionality and in particular a solution whereby discs would be encrypted as well as being introduced to the evidential chain. The Record Retention Policy for such discs should this functionality be available would be as per current Force procedures i.e. For Serious Crime 12 years* and standard crime 6 years* (*Case assessment may initiate further retention).

The Cyber Kiosk cannot add delete or amend data. It is a forensic read only tool that allows for the information to be gleaned from the device in a manner that is proportionate to the needs of the enquiry.

Authority to commence with examination

To clarify police will seize and examine an electronic device under the authority of a judicial warrant, powers at common law or statutory power when in any of the aforementioned circumstances it is lawful for them to seize and examine that device. A person may also voluntarily provide their electronic device in the knowledge that it will be examined for evidence (relating to that particular crime under investigation). As with any item which is provided to the police voluntarily for examination the consent in this context can be withdrawn

Conclusion

In conclusion it is critical that Police Scotland stands ready and equipped to Police in a digital age. We exist, live and work in a digital environment which sees individuals owning and accessing a multitude of devices. As a consequence although for the majority crime per se has not changed the environment or how it is committed increasingly has some form of digital component. It is imperative that Police Scotland embraces new technology to advance how we investigate crime and keep people safe.

If I can be of any further assistance please do not hesitate to contact me.

Nicola Burnett
Superintendent
Specialist Crime Division
6 June 2018

Appendix A - Telephone Kiosk Trial

Memorandum

Date: 19th September 2016

** redacted under Section 30 (c) - Prejudice to the Effective Conduct of Public Affairs.

** redacted under Section 33(1) (b) - Commercial Interests and the Economy.

Telephone Kiosk Trial
E Division CID
10/05/2016 – 02/09/2016

Between 10/05/2016 and 02/09/2016 ** E Division ** trialled the use of

** redacted under Section 33(1) (b) - Commercial Interests and the Economy.

This computer terminal situated in the CID Proactive office at ** E Division ** allows trained users to conduct examination and download of the content of a mobile phone and/or SIM card.

** redacted under Section 33(1) (b) - Commercial Interests and the Economy.

Training was provided at the outset of the trial and 25 users from across all CID disciplines in E Division were trained.

Over the trial period a total of 195 mobile phones and 262 SIM cards were examined using the terminal. The figure of 195 mobile phones represents the approximate amount of mobile phones examined by SCD cybercrime east,

** redacted under Section 35 (1) (a) & (b) – Law Enforcement and Section 34(1)(b) - Investigations

per month, approximately 8% of their annual turnover. Of the 195 phones and 262 SIM cards examined, a negligible amount is thereafter sent on to cybercrime for any further examination. Cybercrime has noted a marked decrease in the amount of examinations requested during similar periods.

The terminal provides the facility to export data on both PDF and Excel documents and also allows data to be exported to a USB saving on the cost of repeatedly downloading to disk. It also allows the users to carry out their own research, searching previously downloaded phones for names, number etc of interest to ongoing enquiries. The terminal has the capacity to download the majority of phones on the market and the list will increase with regular software updates. From an oversight point of view the terminal Admin user can see a report of all activity on the machine to ensure it is being used correctly and within the authorised parameters.

** redacted under Section 35 (1) (a) & (b) – Law Enforcement and Section 34(1)(b) - Investigations

One of the major advantages of the trial identified by users was effect of initial engagement with witnesses and complainers. Investigating officers often call on the good will of witnesses to surrender their mobile phones in order to assist enquiries.

Many are understandably reluctant. Use of the ** redacted under Section 33(1) (b) - Commercial Interests and the Economy terminal on many occasions allowed evidence to be captured quickly and phones returned to witnesses immediately. This has helped build trust and cooperation in certain enquiries and is particularly important when dealing with vulnerable victims and victims of violent or sexual offences where there is an ongoing risk to their safety.

In the four month trial period use of the terminal for mobile phone examination has proved integral in the following enquiries:

** redacted under Section 35 (1) (a) & (b) – Law Enforcement and Section 34(1)(b) - Investigations

** redacted under Section 33(1) (b) - Commercial Interests and the Economy.

Submitted for your consideration.

** redacted under Section 30 (c) - Prejudice to the Effective Conduct of Public Affairs.

Appendix B - Kiosk - Trial Business Case

Introduction

This document describes a trial undertaken by the Police Service of Scotland that allowed for the forensic examination of mobile telephones to be undertaken locally as part of a triage process, with evidentially useful items being forwarded to the appropriate Cybercrime hub for full examination and evidential processing.

The reason for this trial being undertaken was to establish whether such an arrangement was practical and to measure the time saved by Cybercrime by not having to examine every device seized.

Background

Mobile phone examinations form a substantial part of the workload undertaken by the Cybercrime Units of the Police Service of Scotland. Each year over ten thousand mobile phones, SIM cards, tablets, and mobile storage devices are examined[1], with an average of only 4% being used evidentially after examinations have been completed.[2]

The situation has changed drastically over the years. At one time it was possible to examine all data from a mobile device within a matter of only a very few minutes, with the greatest possibility of all data being located on the device's associated SIM card. This data could be printed out onto only a few sheets of paper and presented as is as a court production.

The enormous movement in mobile technology in the intervening years has seen this simplicity eliminated almost completely. Smartphones now comprise over 90% of the devices submitted for examination, with which arrives numerous other impediments: they have enormous data capacities, enhanced security features, a wide variety of styles and systems, and have a vast range of applications available for them, all of which can hold different data that requires processing in different ways. Indeed, by the sheer variety of storage capacities, operating systems, handset makes and models and application software, it is entirely true to assert that mobile examinations are *at least* as complex as computer examinations, if not more.

Smartphones

The market for Smartphones is huge. In the UK alone it is estimated that there at 42 million Smartphone users[3][4] with this number growing every year. Smartphones are released at an increasing rate every year; Samsung alone released 56 new models in 2014[4] with other manufacturers not far behind, and with companies such as Xiaomi and Huawei flooding the Western market with products formerly intended for the Far East. In short, the number of Smartphones is such that it is unusual for a Cybercrime investigation of almost any type not to include at least one Smartphone, if not many.

[1] The actual figures for mobile examinations alone in 2015 are 3513 for Glasgow and the west, 2556 for Edinburgh and the east, 1723 for Dundee and Tayside, 834 for Inverness and the north, and 1934 for Aberdeen and the north east, giving a total of 10560 devices. Source: local databases held by legacy examination units.

[2] Source: local databases held by legacy examination units.

[3] Source: Statista UK https://www.statista.com/statistics/270821/smartphone-user-in-the-united-kingdom-uk/

[4] Source: Wall Street Journal, 17th November 2014, "Samsung Plans to Reduce Smartphone Models by Up to [4] %"

This places an undue burden on Cybercrime Units. Whereas it is true to say that examination techniques have improved significantly in recent years, it is also true to say that the number of Smartphones submitted has caused a considerable strain on Cybercrime's ability to deliver a suitable extraction production in a timeous manner.

**** redacted under Section 35 (1) (a) & (b) – Law Enforcement and Section 34(1)(b) - Investigations**

A better option would be to provide a system that allows officers to extract their information locally and to assess for themselves whether or not a device is worth sending to Cybercrime for examination, whether by assessing its content, ownership or even if it is working or not. By doing this, a reduced number of devices can be submitted to Cybercrime which in turn frees up time for the analyst to carry out examination of the 'useful' devices using the various technical and analytical tools that they have at their disposal. By doing this, Cybercrime benefits by having fewer devices to examine which produces a reduced backlog and the enquiry officer benefits by having a faster response to his or her enquiry using a trained analyst using the available forensic tools.

It was therefore felt that a trial of this system was warranted.

Commercial Solutions

**** redacted under Section 33(1) (b) - Commercial Interests and the Economy.**

**** redacted under Section 35 (1) (a) & (b) – Law Enforcement and Section 34(1)(b) - Investigations**

Trial Implementation

Permission was granted by the Force Executive to trial

**** redacted under Section 35 (1) (a) & (b) – Law Enforcement and Section 34(1)(b) - Investigations**

- The examinations being carried out would only be allowed on summary cases. Any other examinations would have to be sent to Cybercrime East.[5]
- Examinations would be collated for statistical analysis.

Given the above conditions, unit staff was encouraged to examine phones for not only their own departments but for others requesting help from outside. Support was also offered from Cybercrime should any difficulties arise.

The trial ran from 10th May 2016 to 2nd September 2016.

Outcome of Trial

On conclusion of the trial the results were collected by Cybercrime (East). **** redacted under Section**
35 (1) (a) & (b) – Law Enforcement and Section 34(1)(b) - Investigations

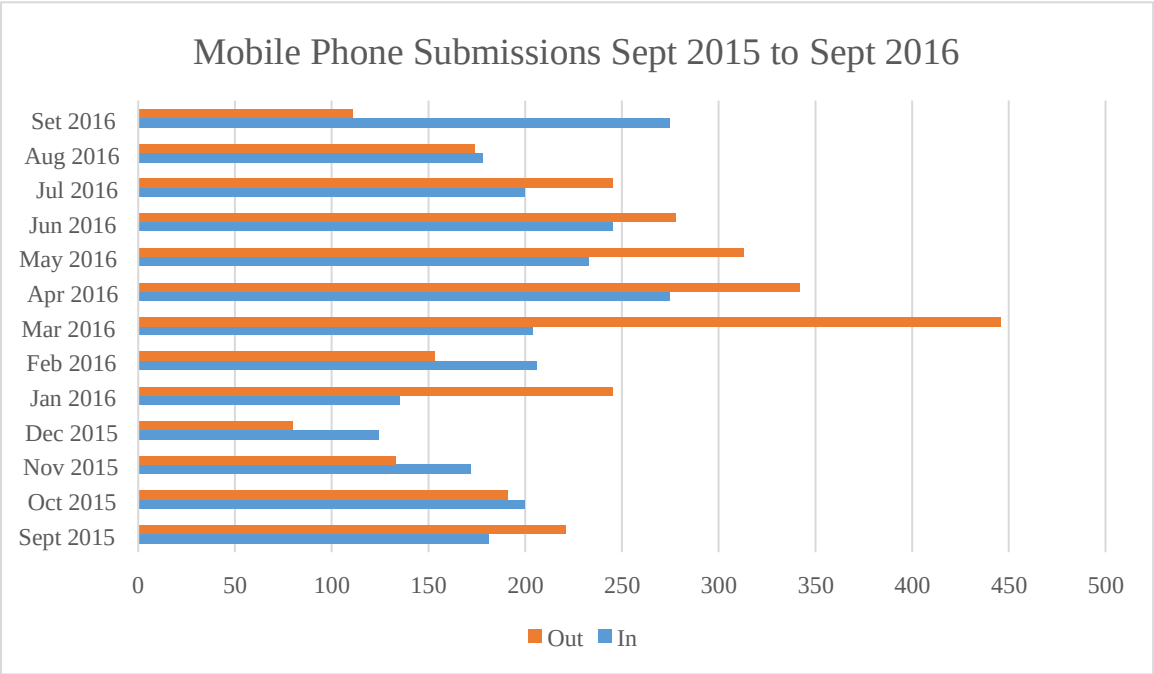
[5] This point was made very strongly on behalf of the Force Executive.

However, the overwhelming result of the trial from **** redacted under Section 35 (1) (a) & (b) – Law Enforcement and Section 34(1)(b) - Investigations**

was that it was successful.

They reported examining 195 mobile telephones and 262 SIM cards and passed on to Cybercrime a 'negligible amount'. This has positively reflected upon the submissions made to Cybercrime East during this period, as the following graph shows, where submissions can be seen to fall between May and August 2016, sharply increasing in September 2016:

Footnote 6 - ** redacted under Section 30 (c) - Prejudice to the Effective Conduct of Public Affairs.



The figures given represent approximately 8% of the yearly submissions made to Cybercrime East.[6]

Advantages

To consider the advantages offered by this project, we can consider the following.

- The average time taken for Cybercrime East to process a phone case for a mid-ranged case on our priority matrix is approximately eight weeks.
- The process which we employ for such a case is to extract all data on the handset(s), write it to DVD and return that to the reporting officer to ascertain what data if any is required evidentially. The officer then has to manually go through the extracted data and revert to Cybercrime for an evidential report.

This clearly is a lengthy process which only introduces delays to the speed at which cases are being dealt. Further, due to the fact that Cybercrime have to examine every phone submitted

[6] It is assumed that the 262 SIM cards would be accounted for within some proportion of the 195 phones submitted.

it follows that the turnaround time is inversely proportionate to the backlogs that this process causes.

A more profitable solution would be to allow divisions to examine their own handsets and decide what is and what is not evidential, then issue clear instructions to Cybercrime for the full examination and extraction of the phone data. This would allow cases to be dealt with far more quickly than they are at present and would enhance the services offered by Cybercrime by allowing a greater time to be spent on more complex cases, where the use of full analytical tools can be used instead of assuming that the reporting officer can do it all manually. This in turn will allow us to have a faster service with far fewer lost opportunities to gather evidence and intelligence. It would also allow enquiry teams to read phones immediately prior to interview, which has long been seen as significantly advantageous.

Another benefit to this revised process is to allow the early return of witness' phones by allowing their content to be read by the enquiry team, as opposed to queuing it for examination with Cybercrime. Following on from this, this process will also allow for the early elimination of suspects from the enquiry.

Disadvantages

**** redacted under Section 35 (1) (a) & (b) – Law Enforcement and Section 34(1)(b) - Investigations**

This brings about another potential issue, in that officers may be reluctant to examine anything as they are likely to be unable to determine from the outset what cases are likely remain at summary level. In effect, this is what prevented the officers **** redacted under Section 35 (1) (a) & (b) – Law Enforcement and Section 34(1)(b) – Investigations** examining more devices. That, however, is a training issue which can be addressed.

Training

Training for the pilot schemes was provided by **** redacted under Section 33(1) (b) - Commercial Interests and the Economy** attending and giving briefings to the officers who were to be accredited with the use of the kiosks. The essence of the kiosk is that it is simple to operate; there is no need for a formalised course extending over a number of days. It can be comfortably taught in well under an hour.

Other Forces

Other UK Forces were consulted for their opinions on the suggested system. **** redacted under Section 30 (c) - Prejudice to the Effective Conduct of Public Affairs.**

Indeed, this is the reason why the Kiosk product was developed.

In canvassing the opinions of other digital forensics managers in the UK it was found that they have a number of different practices, ranging from a wide degree of 'divisional outsourcing' to keeping all examinations completely in-house within their Cybercrime Units.

The location where the kiosks were to be situated was less of an issue. With only two exceptions, everyone who responded to my enquiry replied that they did *not* keep the kiosks in Custody Suites and had no intention of doing so. They expressed a lack of enthusiasm at

keeping that type of device in a public area, preferring to retain them at divisions where enquiry officers can use them.

Without exception, all persons responding indicated that the process was tightly managed by their Cybercrime Unit management and that some of them dip sampled the extracted product to test the quality of the process.
**** redacted under Section 30 (c) - Prejudice to the Effective Conduct of Public Affairs.**

Recommendations
Given the foregoing, the project gives us the opportunity to speed up the overall phone examination process and thereby free up Cybercrime staff for fuller analysis of other cases. There will also be a corresponding reduction in phone examination backlogs which will allow Cybercrime staff to focus on other types of enquiry. The other benefits are that it allows for early results of enquiries to be known by enquiry teams, allows for witness' phones to be returned timeously and allows for the elimination of suspects at an early stage.
**** redacted under Section 33(1) (b) - Commercial Interests and the Economy.**

Submitted for your consideration.
**** redacted under Section 30 (c) - Prejudice to the Effective Conduct of Public Affairs.**

Appendix C – All Emails Redacted

-----Original Message----- Sent: 04 January 2017 11:44

From COPFS
Subject: Telephone Kiosk Pilot [NOT PROTECTIVELY MARKED]
Happy New Year
Have canvassed round staff in the offices covering E&J Divisions. No particular comments other than anything which speeds up the process would be most welcome.
I'm happy to canvass nationally round COPFS if that is required, but would need something to explain the process to colleagues who would be unfamiliar with what a "telephone kiosk" would do.

-----Original Message-----

Sent: 20 December 2016 14:51
From COPFS
Subject: RE: Telephone Kiosk Pilot [NOT PROTECTIVELY MARKED]
I'm canvassing round the offices for any feedback or observations staff may have.
Unfortunately not the best time in the year to do so.
Will get back to you when I've heard back but if you need a reply sooner just send me a reminder.

-----Original Message-----

Sent: 07 December 2016 12:35
TO COPFS
Subject: FW: Telephone Kiosk Pilot [NOT PROTECTIVELY MARKED]
I hope this email finds you are well? Can you recall the pilot I ran for Telephone Kiosks in the East within E and J Divisions?
The project concluded a few months back and to be honest has established excellent results in E Division and mixed results in J Division.
That being said the opportunities for use did assist and I would suggest found in favour of wider use of the products on trial.
You will see from the email stream below that **** redacted under Section 30 (c) - Prejudice to the Effective Conduct of Public Affairs.** is seeking to purchase kit for the Divisions use. I have no issue with this provided there is oversight and training supplied by Cyber Forensics managed through the Division to ensure compliance with the forensic principles, the updating of equipment and staff and appropriate governance around the product ensuring a consistent approach.
Do you have a view on the use of such technologies at the frontline given the clear benefits that we established in E Division.
I genuinely believe this is the way forward minimising the time phones are retained and returned to witnesses and victims which in turn reduces claims against PSoS and CAP.
Your thoughts on how to take the matter forward would be appreciated.
Best regards.

-----Original Message-----
Sent: 06 December 2016 16:37
Subject: RE: Telephone Kiosk Pilot [NOT PROTECTIVELY MARKED]

Sorry about the delay getting back to you.
**** redacted under Section 30 (c) - Prejudice to the Effective Conduct of Public Affairs.**

Hope this helps

-----Original Message-----
Sent: 02 December 2016 07:30
Subject: Re: Telephone Kiosk Pilot [NOT PROTECTIVELY MARKED]
So I take it E div would be unable / or not permitted to progress this until the capital bid is approved / declined? The nationwide delivery of telephone kiosk would be fantastic but I'm keen to provide feedback / a solution to the teams who benefited from the pilot as it enhanced our operating model and worked.
Thanks

----- Original Message -----
Sent: Thursday, December 01, 2016 09:22 PM
Subject: Re: Telephone Kiosk Pilot [NOT PROTECTIVELY MARKED]
Kiosk forms a part of a broader cyber bid that has been submitted to the executive. The contents of the bid have been recognised and highly prioritised by the Executive and now await approval from SPA and SG.
The timescales for approval and funding are not clear. We had hoped for funding this financial year but may well spill into 2017-18. When I have a definitive update I will let you know.

----- Original Message -----

Sent: Thursday, December 01, 2016 09:15 PM
Subject: Re: Telephone Kiosk Pilot [NOT PROTECTIVELY MARKED]
The Capital bids are in and sitting with DCC Gwynne.
DSU Cravens is pursuing the bids on our behalf through DCS McLean.
I suspect the conversation needs to be developed at your level.
As indicated I believe they should be rolled out across the Force but this needs the blessing of the FE with strict TOR.
DSU Cravens would you like to offer comment?
Happy to assist where I can.

----- Original Message -----

Sent: Thursday, December 01, 2016 08:47 PM
Subject: Re: Telephone Kiosk Pilot [NOT PROTECTIVELY MARKED]
Can you discuss this with **** redacted under Section 30 (c) - Prejudice to the Effective Conduct of Public Affairs.**

What is the timescale for the capital bid and the kit being issued to the divs. This has been a great success in the division and I am keen to re-establish / set - up. Can we do another trial period or obtain on a short term hire if the capital bid is going to take sometime
Thanks

----- Original Message -----

Sent: Friday, November 11, 2016 12:16 PM
Subject: RE: Telephone Kiosk Pilot [NOT PROTECTIVELY MARKED]
In answer to your questions:
**** redacted under Section 33(1) (b) - Commercial Interests and the Economy.**

**** redacted under Section 30 (c) - Prejudice to the Effective Conduct of Public Affairs.**

Of interest to you is that any IT purchases that are to be made have to go through Martin Low and his team at ICT. Further I have made a capital bid for this equipment for all divisions across Scotland.
CH Supt Cuzen allowed this trial on the basis that we provide a report for consideration in a business case for the FE to consider. This has recently been superseded by the Capital Bid requested by DSU Cravens who now is leading on the capital bid for this equipment. I raise this as any deployment of kit would have to be managed by the Cybercrime Forensics with tight controls and training.
**** redacted under Section 30 (c) - Prejudice to the Effective Conduct of Public Affairs.**

Whilst I fully support and recommend its deployment in the field given our significant success in E Division, it would not be helpful for Divisions to 'go it alone'.
Hope this aids the conversation.
Best regards.

-----Original Message-----
Sent: 11 November 2016 12:02
Subject: Fw: Telephone Kiosk Pilot
Is there any chance you can answer the questions the DSu has asked me re the costs?
Cheers

----- Original Message -----

Sent: Friday, November 11, 2016 11:36 AM
Subject: FW: Telephone Kiosk Pilot
Thanks
**** redacted under Section 33(1) (b) - Commercial Interests and the Economy.**

- can you include this in the memo? But I intend to progress with the Commander just now.
Thanks

-----Original Message-----
Sent: 27 September 2016 07:44
Subject: Telephone Kiosk Pilot

D/Su
Please find attached memo outlining the benefits experienced by the division during the recent pilot of the **** redacted under Section 33(1) (b) - Commercial Interests and the Economy** telephone kiosk terminal.
I have circulated the memo to all DI's prior to submission to you and the only comments to come back are to emphasise the benefits that quick download of mobile phones has on quickly identifying suspects in sexual crimes and the ability that gives the SIO to quickly direct resources and prioritise enquiries. That can be reflected across all the CID disciplines.

Please note that **** redacted under Section 33(1) (b) - Commercial Interests and the Economy.**

Please let me know if there are any questions or anything you wish expanded on in the body of the memo.
Thanks
NOT PROTECTIVELY MARKED

E-MAIL TRAIL ENDS

----Original Message----- Sent: 14 April 2017 08:31
Subject: FW: Telephone Kiosk Pilot [NOT PROTECTIVELY MARKED]

**This email has apparently never arrived with you!! Can you draft a one pager for **?
Please return to me for forwarding on.

** can you draft a page on the kiosk and the benefits of its use in order that ** can canvass support across the country for its deployment?

----- Original Message -----
Sent: Wednesday, February 15, 2017 11:39 AM
Subject: RE: Telephone Kiosk Pilot [NOT PROTECTIVELY MARKED]
From COPFS

Happy to do so. Is there something, relatively brief, explaining how it would work and the benefits that I can circulate round?

-----Original Message-----
Sent: 10 February 2017 08:33
To: COPFS
Subject: RE: Telephone Kiosk Pilot [NOT PROTECTIVELY MARKED]

**** redacted under Section 30 (c) - Prejudice to the Effective Conduct of Public Affairs.**

-----Original Message----- From: COPFS
Sent: 20 December 2016 14:51
Subject: RE: Telephone Kiosk Pilot [NOT PROTECTIVELY MARKED]

I'm canvassing round the offices for any feedback or observations staff may have. Unfortunately not the best time in the year to do so.

Will get back to you when I've heard back but if you need a reply sooner just send me a reminder.

E-MAIL TRAIL ENDS

-----Original Message----- Sent: 24/02/2017

Here it is.

We may know something in the next week or so. Even if you wanted to procure it would not be bought and on premises in time for the financial year end and therefore not purchasable on this year's budget. ** is hopeful for a positive outcome and another month at worst will see the direction of travel.

Hope this helps.

E-MAIL TRAIL ENDS