Justice Sub-Committee on Policing

Police Scotland’s digital data and ICT strategy

Written submission from Police Scotland

The following information is provided for information of the Justice Sub-Committee.

ICT

As a result of the non-delivery of the i6 programme, the technology transformation of legacy ICT platforms that support core operational policing remains an outstanding issue that continues to present challenges in relation to the Force’s data, information management and business process efficiency, which in turn affects operational effectiveness. In order to address these challenges and deliver on our 2026 strategy objectives, it is essential that the Force has credible and robust, vision, strategy and delivery plans in relation to Digital, Data and ICT, including a plan to address the continuing legacy of i6 non-delivery.

Our approach to technology delivery post i6 is to drive delivery within the overall 2026 Strategy, with Police Scotland placing the learning from i6 non-delivery at the very centre of our decision making processes, when considering options for our approach to future delivery. Given the pressing need to replace a range of legacy policing systems and the commensurate desire to minimise risk of non-delivery, the design principles underpinning our planning emphasise an approach which will be modular, iterative and agile, with a strong preference towards the re-use or re-development of proven technologies, as opposed to the delivery of a single, new, all-encompassing solution procured from one particular supplier.

In support of the technology objectives laid out as part of 2026, the Digitally Enabled Policing Programme (DEPP) has been established as the vehicle to support delivery of relevant technology solutions, with ACC Malcolm Graham being appointed Senior Responsible Officer. Within the DEPP, the i6 footprint will be addressed through the Core Operational Solutions (COS) sub-programme and this sub-programme is currently engaged in compiling an Initial Business Case which defines the scope of works required to address the ongoing issues around i6 non-delivery.

The COS Initial Business Case is scheduled to be considered by the Police Scotland Change Board, on 1st May 2018. Subject to approval, the COS sub-programme will then begin implementation of Phase 1, which will be the delivery of the following modules:

- National Missing Persons module
- National Productions module
- National Federated Search module (allowing single search across multiple data sources)
- National Road Traffic Collisions module
- Linkage of our Vulnerable Persons system to the UK Police National Database.
Phase 1, is planned to complete within the first year of the programme and will enable early progress to be made in establishing the overall solution enterprise technology ‘ecosystem’, whilst delivering on those modules that are most time critical to the Force. Thereafter, phase 2 will comprise deliver of the major operational modules supporting Crime, Enquiries and Case management. Finally Phase 3 will deliver those modules which represent remaining added value, including the integration of standalone national applications, such as our newly introduced national Custody Solution (NCS). Overall it is envisaged that these 3 phases will be delivered within a 3 year period.

Investment of the £4.94 million in capital has been set aside for 2018/19 for the COS sub-programme area.

In addition to engagement within internal stakeholders, the Initial Business Case has been reviewed by colleagues from Scottish Government Digital Transformation Services, with feedback being acted upon to ensure that the proposed approach is aligned with wider Government and Criminal Justice Digital Strategies. The pace of development of the COS Initial Business Case has also been adjusted to ensure it is in alignment within the newly developed Police Scotland Digital, Data and ICT Strategy.

While a draft ICT Strategy was developed some time ago, Police Scotland recognised that in order to drive forward delivery of the objectives set out in our vision for 2026, it was necessary for us to have a joined up approach to Digital, Data and ICT strategy across the organisation. But it was also identified that the Force did not have sufficient in-house capacity to undertake the work required to deliver the a strategy for Digital, Data and ICT within the necessary timescale and therefore, with the support of SPA, the Force decided to engage with external Professional Service providers to deliver the necessary products that would allow the Force Executive to make informed decisions in relation to addressing the challenges outlined above.

At the end of 2017, an Invitation To Tender (ITT) process was undertaken in order to select a professional services provider who had the necessary capability and experience to help the Force define and deliver the required products and as a result of this process Ernst & Young were engaged to undertake the work to deliver the following key products:

1) A Digital, Data and ICT strategy
2) A Strategic Outline Business Case (SOBC) for the delivery of the strategy objectives
3) A series of 100 day plans that detail the work necessary to advance the project to Outline Business Case (OBC) and further detailed planning

Ernst & Young have now produced the required documents, including the combined Digital, Data and ICT strategy. These products have been reviewed and approved by both the relevant project governance group and the Force Executive and will be submitted to the SPA Board for review/approval on 31st May 2018. Thereafter, further development of the Digital, Data and ICT strategy and proposals for its delivery will be taken forwards in accordance with existing PSoS, SPA and SG governance procedures.
Digital device triage system – cyber kiosks

Digital Device Triage System are often referred to colloquially as cyber kiosks. Contrary to recent commentary by others, Police Scotland does not currently employ such devices operationally as there are ongoing matters of policy, planning and training still being finalised. In furtherance the purchase and potential introduction of such devices operationally has been considered as part of the ongoing transformation of the service – Policing 2026.

The size and complexity of mobile devices being submitted over the years has seen a dramatic increase. At one time it was possible to examine all data from a 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 a court production. Over the last year approximately 40,000 mobile devices were seized by Police Scotland. Only a small proportion of these are submitted for digital forensic examination.

The exponential growth in the size and complexity of mobile technology in the intervening years has seen the simplicity eliminated almost completely. Over 90% of the devices submitted for examination relate to Smartphones with which come numerous other technical challenges: 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. Nevertheless these applications represent fantastic investigative opportunities.

In the UK alone it is estimated that there are 42 million Smartphone users with this number growing every year. Smartphones are released at an alarming rate every year; Samsung alone released 56 new models in 2014 with other manufacturers not far behind, 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 criminal investigation of almost any type not to include at least one Smartphone, if not many.

In keeping with Policing 2026 and digitally enabling frontline officers and enhancing cyber and forensic capabilities, Police Scotland Specialist Crime Division Cybercrime Unit anticipate deploying later this year, a system of triage which allows officers to make a very early assessment of which mobile devices require to be examined more fully. The extraction of information locally provides a quick time assessment as to whether or not a device is evidentially meaningful before sending to Cybercrime for examination.

Key information will enable accurate records to be maintained of who has examined what, when, and why. Only user logs will be retained on the actual systems for audit purposes.

There are two market leading products that facilitate triage assessment of mobile devices (MSAB and Cellebrite) both provide a triage tool for examination of mobile devices. These devices have the appearance of a small desktop computer with a
touch screen, rather than some mysterious piece of kit utilised behind a screen which unfortunately, the industry term of ‘Kiosk’ suggests. Following a procurement process Police Scotland have selected the Cellebrite product and anticipate rolling out 41 kiosks across the force area.

This is effectively an improved and modern system of triage. The potential to deploy such devices at the front end of policing provides an opportunity to reduce unnecessary device retention consequently reducing unnecessary backlogs in devices awaiting full digital forensic examination. Critically service to the public will be improved as such triage can assist in reducing undue delay by returning negative/unneeded devices.

In 2016 Police Scotland conducted trials of the Cellebrite Digital Device Triage System. The trials in Edinburgh and Stirling related to devices in relation to less serious offences i.e. potential for evidence to be considered in summary procedure. These trials saw several hundred devices triaged with a minimal amount requiring further digital forensic examination.

Learning from trials and colleagues elsewhere in UK Law Enforcement supports the introduction of such devices.

With regard to data protection & retention, when the police seize an electronic device under the authority of a judicial warrant, statutory power or following a suspect’s arrest, it is lawful for them to seize and examine that device for evidence. 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).

Data identified as relative to a Criminal Investigation will be subject to the Force existing data retention policies which are 6+1 Years for Minor Crime and 12 +1 for Serious Crime.

The advantages and benefits of the operational deployment of such devices are:-

- Reduced submissions requiring digital forensic examination – currently this can take up to 8 months.
- Enhanced service to public as many devices are returned at much earlier stage.
- The aforementioned therefore provides that specialist resource can increase time spent in the investigations of serious and complex cases, maximising public protection and accelerating investigations all to the benefit of the public.
- The opportunity to triage devices at initial stages of an incident or enquiry will support the service provided to victims, witness as well as suspects and accused.

Police Scotland continue to consider all aspects of policy, planning and training thus providing an assurance that operational deployment of such devices is supported by a robust and informed framework. This will include the submission of an Equality and Human Rights Impact Assessment and Privacy Impact Assessment before operational deployment.
It is the intention of Police Scotland to link in with key stakeholders which will include a ‘show & tell’ of the device and provide an opportunity to discuss proposed policy, planning and training.

This facility is an essential tool in the cyber approach to protecting victims and keeping people safe. It is in essence a triage tool which does not retain permanently any viewed data.

Use of ‘iris recognition’

Facial recognition within policing across the world has become a topical issue over the last 12 months, with news stories such as the police in China using facial recognition embedded into CCTV to identify and capture a criminal in a crowd of 60,000 within 5 minutes. In a more realistic context, this innovation could prove extremely useful to Police Scotland and in particular within its custody facilities.

Using iris scanning techniques would, in theory, reduce queue time, reduce the time custody officers spend form-filling, and quickly identify repeat visitors. The benefits of this are obviously clear however facial recognition presents considerable risk if implemented poorly without the proper consultation and funding. Despite this, it has been successfully integrated into other sectors – such as aviation, where it is now common practice to use iris-scanning at passport barriers and some forces in England and Wales are already using a form of this technology.

The idea could also bring great benefit to the most vulnerable people within Police Scotland’s custody system – these individuals would be easier to identify and officers would have more time to understand their unique situations. Iris scanning has also been proven to generate more accurate results than other biometric methods, such as fingerprint identification.

Police Scotland are considering this technology along with other ITC solutions as highlighted by Chief Superintendent Garry McEwan, Criminal Justice Services Division at the evidence session on Thursday 19th April 2018. This will be subject to rigorous scoping and optional appraisals in the forthcoming 12 months.

Police Scotland
30 April 2018