SCOTTISH POLICE AUTHORITY

Agenda Item 8

Meeting	**Authority meeting**
Date	**20 May 2020**
Location	**Video-conference**
Title of Paper	**Digital Forensics Working Group Report**
Presented By	**Robert Hayes, SPA Board Member**
Recommendation to Members	**Endorsement of Recommendations**
Appendix Attached	**Yes – DFWG Report**

PURPOSE

The purpose of this paper is to:-

To present the Report of the Digital Forensics Working Group for Board consideration, agreement of the Recommendations of the Report, and noting of the additional work required.

1. BACKGROUND

1.1 On 26 June 2019, I was asked by the Scottish Police Authority (SPA) Board to chair a short life Digital Forensics Working Group (DFWG) to review the delivery, accreditation, oversight and governance of digital forensics in Scotland. The target for the group was to deliver a report to the Forensic Services Committee of the SPA by the end of April 2020.

1.2 The DFWG Report was considered by the SPA Forensic Services Committee on the 20th April 2020, and all the recommendations accepted and agreed. As the scope of the report is wider than the Forensic Services Committee, it was referred to the SPA Board for consideration and decision in relation to the recommendations.

1.3 The Report of the Working Group which is attached as Appendix A, is the product of much work across the agencies involved, and sets out clear recommendations. I commend it to the committee.

2. STRATEGIC IMPLICATIONS

2.1 The current Police Scotland / SPA 10 year strategy for policing "2026 Serving a Changing Scotland" has "Enhance cyber & forensic capabilities" as a strategic objective. As the Report clearly articulates, the gap between capability and true demand has, and is continuing to grow.

2.2 Citizens in Scotland increasingly communicate, shop, bank, and manage their affairs online. Criminals from all parts of the globe are exploiting the opportunity to commit crime remotely. Despite internet service providers filtering out almost 95% of attempts, most users still receive phishing attempts on a daily basis.

2.3 Police Scotland and the wider criminal justice system have a duty to respond to this changing world, and continue to prevent & detect crime, whether physical or technology enabled.

2.4 Failing to adapt to the realities of our connected world will have performance & reputational issues for Police Scotland, the SPA, and the broader criminal justice system.

3. FINANCIAL IMPLICATIONS

3.1 It is clear that the broader issue of digital forensics, and the associated exploitation of digital evidence and intelligence is

significantly under-resourced. It is expected that the emerging Police Scotland Cybercrime & Technical Surveillance Programme will require significant funding to prevent Police Scotland falling further behind.

3.2 Accrediting digital forensics within a well-defined Quality Framework is essential for reasons which are well articulated in the report. There will be a significant cost to achieve this.

4. PERSONNEL IMPLICATIONS

4.1 Current staffing and budget is simply not meeting current demand, and it is clear that demand is rising exponentially, both in scale and complexity.

4.2 It is essential that Police Scotland's developing Workforce Plan reflects the numbers of staff and skills profile that will be needed for Police Scotland to effectively manage this critical area of policing.

4.3 It is essential that Police Scotland's developing Workforce Plan reflects the numbers of staff and skills profile that will be needed for Police Scotland to effectively manage this critical area of policing.

5. LEGAL IMPLICATIONS

5.1 Options that would require legislative change are not recommended in the report, otherwise there are no direct legal implications associated with this paper

6. REPUTATIONAL IMPLICATIONS

6.1 Reputational implications are articulated at Section 2 of the report.

7. SOCIAL IMPLICATIONS

7.1 There are no social implications associated with this paper.

8. COMMUNITY IMPACT

8.1 There are no community implications associated with this paper.

9. EQUALITIES & RIGHTS IMPLICATIONS

9.1 In our connected world, devices such as mobile phones and tablets contain snapshots of their owner's lives, relationships, and history. Exploiting the evidential & intelligence opportunities of this data needs to be done within a clear rights based framework. As the report highlights, there is a need for a mature public conversation that considers the balance between the need to investigate with the rights of the individual, whether they are victim, witness, or offender.

9.2 Understanding these perspectives was an important aspect of the stakeholder consultation events conducted as part of this work.

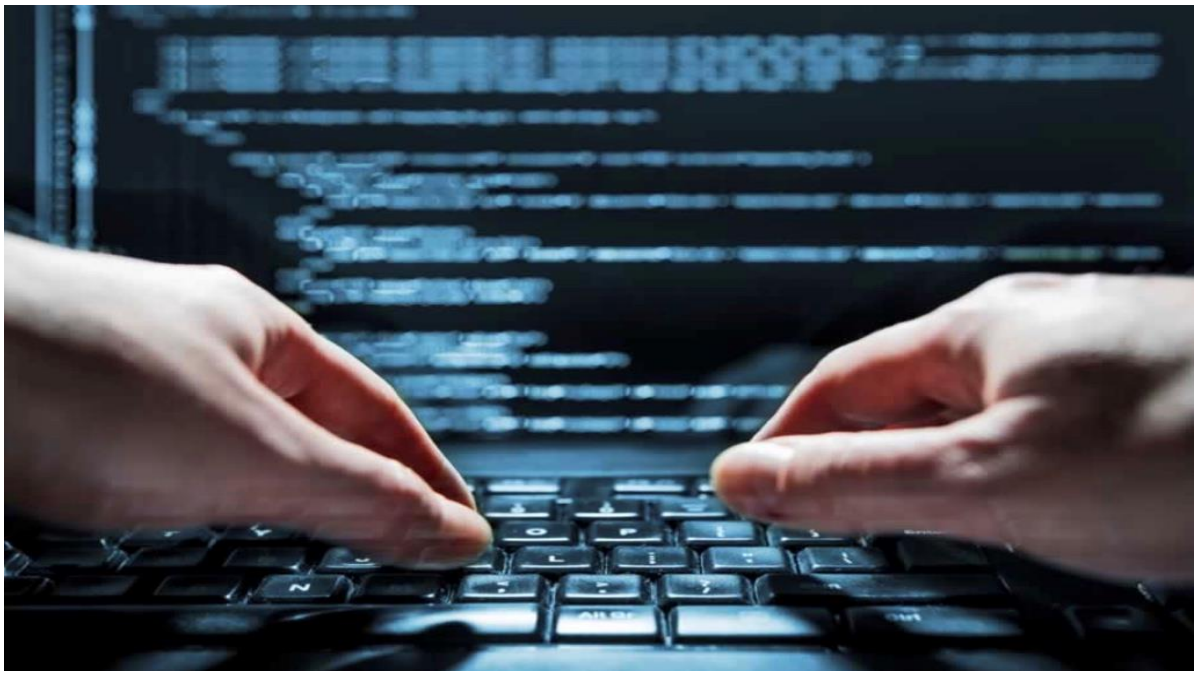
10. ENVIRONMENT IMPLICATIONS

10.1 There are no environmental implications associated with this paper.

RECOMMENDATIONS

Members are requested to:

a) Consider the attached report
b) Agree the report recommendations
c) Note the additional work required



A report to the SPA Forensic Services Committee: on options for the future delivery, accreditation, oversight and governance of digital forensics in Scotland.

SPA Digital Forensics Working Group (DFWG)

April 2020

Table of contents

Appendices

Foreword

On 26 June 2019, I was asked by the Scottish Police Authority (SPA) Board to chair a short life Digital Forensics Working Group (DFWG) to review the delivery, accreditation, oversight and governance of digital forensics in Scotland.

The present review comes at an opportune moment as it allows the position on digital forensics in Scotland to be developed in a principled manner which gives appropriate weight to considerations of public safety and security on one hand, and privacy and other human rights and ethical considerations on the other. Such development should proceed with as much public awareness and engagement as possible, to try to ensure that there is appropriate public confidence and trust in technology and data which will be used increasingly by the police, and which as a consequence is important to everyone in civil society.

From the perspective of knowledge, experience and continuity, we have been fortunate in our work to have as Working Group members several individuals and agencies who were previously members of the Independent Advisory Group (IAG) on Biometric Data in Scotland chaired by solicitor advocate John Scott Q.C. Whilst the use of biometrics and digital forensics for criminal justice purposes in Scotland are distinct, they do of course have many similarities and intersect at various points with identical privacy, human rights and ethical considerations. In that regard, the seminal work of John Scott Q.C. and the IAG on Biometric Data in Scotland, and the work of the Forensic Science Regulator in England and Wales, has been key in informing our own conclusions on the required next steps for digital forensics in Scotland.

We also had the benefits in membership of our Group of considerable knowledge, experience and expertise in the fields of policing, forensic science, criminal justice, data protection, human rights and qualitative research. I am grateful to all for their contributions and should make special mention of my fellow SPA Board Member Jane Ryder who led on our consultation and engagement work with stakeholders. This report could not have been produced in such a short period of time without considerable effort on their part.

The Group first met in September 2019 and had seven months to carry out its work. The final report was completed on 03 April 2020, and its findings, conclusions and recommendations will be considered by the SPA Forensic Services Committee at its meeting on 20 April 2020.

Robert Hayes, Chair of Digital Forensics Working Group

03 April 2020

Executive Summary

The proliferation of digital devices within society, accompanied by the expansion of digital storage and the pace of technological advancement has made digital forensics the youngest, fastest growing, and most evolving area of forensic science. Unlike other forensics, a single digital evidence source such as a smartphone may typically contain more than 1 million individual pieces of data within which important information relative to an investigation may, or may not, exist. This problem of data-overload leaves the digital detective in the unenviable position of metaphorically searching for a needle, or needles, in a haystack.

The sheer volume and complexity of data within devices and storage media has been overwhelming police digital forensic capacity and capability in the UK for some time. This has caused most UK police forces to introduce digital triage devices to help them to determine whether a device or electronic information source may contain inculpatory evidence before sending it for detailed forensic examination. Whilst such triage devices greatly assist in that regard, the rules of disclosure equally require the police to ascertain whether any exculpatory evidence may exist to exonerate the innocent or assist the defence. It has been the failure of the police to do this thoroughly in some high-profile cases in other UK jurisdictions, that has previously called the validity and reliability of the 'science' of digital forensics into question, contributing towards a requirement from the Forensic Science Regulator for police forces and forensic service providers in England and Wales to accredit their digital forensic operations to international ISO quality standards.

Forensic crime scene analysis in Scotland is provided to Police Scotland by SPA Forensic Service to ensure differentiation or a sterile corridor to delineate the police investigation from the scientific investigation. The national Forensic Services model in Scotland from crime scene to court is internationally acclaimed, and places quality and accreditation at the heart of everything. The sterile corridor principle, through differentiation, also exists to exonerate the innocent.

Most of the work of SPA Forensic Service has been accredited to deliver scientific and forensic services by the United Kingdom Accreditation Service (UKAS) for more than 20 years. Third-party assessment by UKAS accreditation offers confidence that forensic activities are carried out impartially and competently. Compliance with the relevant international ISO Standard infers the highest levels of personal conduct, and organisational compliance with quality management systems and standards.

However, digital forensics in Scotland are retained by Police Scotland rather than SPA Forensic Service. Unlike England and Wales, Police Scotland has not yet implemented an overarching Quality Management System (QMS) or sought accreditation for its digital forensics processes, despite a recommendation from HMICS in 2017 that it should consider doing so. This means that Scotland leads much of the UK on forensic science accreditation assurance, but lags with accreditation of digital forensics. This report by the DFWG, engages with these issues by reviewing the delivery, accreditation, oversight and governance of digital forensics in Scotland and making a small number of important recommendations for improvement.

As part of the design of our review, we sought to consider public interest and perspective from the outset. This was particularly important as previous parliamentary criticisms of the cyber-kiosks experience in Scotland had to a large extent focussed on questions of whether there had been adequate external engagement. With that in mind, we engaged widely throughout this review with many stakeholders including the Scottish Information Commissioner, the Children and Young People's Commissioner and the Scottish Human Rights Commission.

During our consultation and engagement, stakeholders felt that digital forensics delivery should remain with Police Scotland but agreed the need for more checks and balances to ensure that the needs of law enforcement are balanced equally with broader privacy and ethical and human rights considerations.

Following an options appraisal and cost vs benefit analysis, we recommend that the delivery of digital forensics in Scotland should remain with Police Scotland under the direction and control of the Chief Constable. There is currently no robust business case in support of an alternative operating model, and to do otherwise at this juncture would require significant financial investment at a time when police finances are already under considerable strain. This decision does not however preclude the future alignment of forensic laboratory work should benefits realisation parameters change as a result of a wider review of all forensic service provision in Scotland.

However, we conclude that Police Scotland should commence a journey of transition to achieve accreditation of its digital forensic laboratory work by December 2022. We also recommend ISO 17025 as the most appropriate quality standard for adoption for the laboratory work, and once accreditation has been achieved, recommend that Police Scotland should voluntarily adhere to the Forensic Science Regulators Codes of Conduct and Practice as mandated for England and Wales. This will place all UK policing forensic sciences on a common platform of requirement for quality standards accreditation.

We also recommend that Police Scotland should conduct a broader piece of work with SPA Forensic Service to develop a quality framework for the non-forensic aspects of digital investigations including triage technologies within the same timescale.

There were some additional matters that arose from our work which were beyond the specific terms of reference and scope of our short life working group. Principal amongst these is the need for significant public investment in the digital space to address some of the longer-term challenges identified in this report. There is also a need for policing, and the wider justice system in Scotland, to better understand the potential trajectory of digital forensics in the years ahead. This will assist in determining optimum modes of transition to medium and long-term operating models, and better address the issues of capacity and capability, particularly in relation to in-sourcing models and decisions.

There is also a need for strengthened internal and external governance around cybercrime, technical surveillance, digital forensics, and digital policing technologies in Scotland to ensure that privacy and ethical and human rights considerations are balanced equally with

the needs of law enforcement. The principles of proportionality and necessity suggest that we should be very careful about the limits of the encroachment we excuse on that basis.

As digital forensics and biometrics raise almost identical privacy, ethical, and human rights concerns, we welcome the work of the Scottish Parliament in passing the Bill to introduce a Scottish Biometrics Commissioner and Advisory Group to support the work of the Commissioner. We view the planned development of a Code of Practice on biometric data by the Scottish Biometrics Commissioner as essential, particularly as digital forensic techniques can sometimes overcome biometric security access controls on certain devices and thus give the police access to highly sensitive personal data, including biometric data. We also welcome the planned Scottish Government Emerging Technologies Independent Advisory Group (ETIAG), and the ongoing Scottish Government work on digital evidence sharing capability (DESC) between criminal justice partners. We view each of these important related developments as useful conduits through which further opportunities for public engagement can take place on the various issues and challenges which arise from policing in a digital age.

Recommendation 1

The delivery of digital forensics should remain with Police Scotland under the operational responsibilities and internal governance arrangements of the Chief Constable.

Recommendation 2

The SPA Board should agree the appropriate Committee(s) to have oversight, scrutiny, and assurance over digital forensics, and the areas covered by the Police Scotland Cybercrime and Technical Surveillance Programme (CTSP).

Recommendation 3

Police Scotland should commence a journey of transition with a view to achieving accreditation for its digital forensic laboratory work by December 2022. It should also conduct a broader piece of work with SPA Forensic Service to develop a broader quality framework for the non-forensic aspects of digital investigations including triage technologies within the same timescale.

Recommendation 4

Police Scotland should adopt the ISO 17025 quality standard for accreditation of its digital forensic laboratory work in Scotland by December 2022.

Recommendation 5

On attaining the ISO 17025 quality standard accreditation for its digital forensic laboratory work, Police Scotland should voluntarily adhere to the Forensic Science Regulators Codes of Practice and Conduct as mandated for Forensic providers, including policing in England and Wales.

Terms of reference

1. On 26 June 2019, the Scottish Police Authority (SPA) Board approved a proposal to establish a short life Digital Forensics Working Group (DFWG) to review the delivery, accreditation, oversight and governance of digital forensics in Scotland. The full terms of reference for the DFWG review may be viewed on the SPA website.[1]

2. The establishment of the short life working group followed on from an earlier thematic inspection of SPA Forensic Services in 2017 by Her Majesty's Inspectorate of Constabulary in Scotland (HMICS). Although HMICS did not formally inspect the delivery of digital forensics by Police Scotland, the thematic inspection report contrasted the formal accreditation and quality standards within forensic science disciplines managed by SPA Forensic Service, with the absence of formal accreditation by Police Scotland in relation to digital forensics. This led to a specific recommendation (Recommendation No 9) that Police Scotland should consider quality accreditation for digital forensics in line with the Forensic Science Regulator (FSR) recommendations, the Home Office Forensic Strategy for England and Wales, and wider good practice in order to support effective public performance reporting and assurance. The 2017 thematic inspection of SPA Forensic Service may be viewed on the HMICS website.[2]

3. This report reflects the findings of the SPA Digital Forensics Working Group following extensive research, consultation, and internal and external engagement over the autumn and winter of 2019/20. Further detail on the composition and membership of the DFWG is included at **Appendix 1** to this report. A list of meetings and consultation and engagement events held is included at **Appendix 2** to this report.

Background to digital forensics and crime

4. Digital forensic science is the process of obtaining, analysing and using digital evidence in investigations or criminal proceedings.[3] There is however a paucity of data in relation to the demand for digital forensics capabilities within UK police forces as the ubiquity of digital devices means that digital evidence may be present in almost every crime.[4] However whilst metrics appear scarce, it is widely accepted that the proliferation of digital devices and technologies is increasing police investigative demand for digital forensic techniques.[5] Digital forensics is a global challenge for policing. Developments in digital investigation progress quickly and present investigators with new challenges constantly. It is

[1] Scottish Police Authority, Digital Forensics Working Group Terms of Reference, 26 June 2019: http://www.spa.police.uk/assets/126884/441011/509407/563684/item10a

[2] HMICS Thematic Inspection of SPA Forensic Service, 27 June 2017: https://www.hmics.scot/publications/thematic-inspection-scottish-police-authority-forensic-services

[3] Digital Forensics and Crime, Houses of Parliament, Parliamentary Office of Science and Technology, Post number 520, March 2016: https://researchbriefings.files.parliament.uk/documents/POST-PN-0520/POST-PN-0520.pdf

[4] ACPO Good Practice Guide for Digital Evidence, Association of Chief Police Officers (2012).

[5] Information for Prospective Bidders, Metropolitan Police Service – Digital Cyber and Communications Forensics Unit (2015).

no longer the question whether, but rather which digital evidence has been left behind at a crime scene.[6]

5. Traditionally, digital forensics mainly involved extracting data from PCs and Laptops.[7] Now, a range of other digital devices and cloud based storage mediums are of importance to investigations including smartphones, Wi-Fi routers, GPS equipment, CCTV, building access recorders, smart TVs, gaming devices, drones, cloud based storage mediums and fitness watches.[8] The most significant area of growth however is in relation to the application of digital forensics to mobile telephones and particularly to smartphones. For example, in 2015, information published by the Metropolitan Police suggested that almost three quarters (75%) of the 40,000 devices that it examines annually were mobile telephones, the majority of which are smartphones.[9]

6. The main goal of digital forensics is to extract data from the electronic evidence, process that data into useful information, and present the findings for prosecution.[10] However digital forensics also has an intelligence function and an exculpatory value and can be used to eliminate innocent persons from police investigations, or assist in other non-criminal justice areas such as missing persons investigations, death enquiries, and matters of national security.

7. Rapid advances in technology means that policing must adapt to the new threats and opportunities for 21st century policing. Online crime continues to grow dramatically, and the internet has provided the opportunity to commit new and borderless crimes. It has also enabled some crime types to be committed on an industrial scale and has facilitated many forms of 'traditional' crime. Some crimes such as revenge pornography and the proliferation of child abuse imagery go largely unrecorded, unanalysed, and as a result, are not fully understood. Criminals are exploiting technology, and the tools to preserve anonymity online, more quickly than law enforcement can harness new investigative technologies. The expectation of Interpol and Europol is that digital and cybercrime will continue to grow exponentially.[11] Digital Policing is a strategic policing priority for the UK, featuring in the National Police Chiefs Council (NPCC) Policing Vision 2025, and in the Police Scotland and SPA Policing Strategies to 2026.

Contextualising the term 'digital forensics' within policing

8. The terms 'digital forensics' and 'digital evidence' are not defined in criminal justice legislation in Scotland or the wider UK, and concomitantly there is no bespoke legal framework catering specifically for digital forensics within policing.

[6] Forensic Big Data Analytics, Netherlands Forensic Institute, forensicinstitute.nl
[7] An examination of Digital Forensic Models. Reich *et al* (2002)
[8] Alternate Data Storage Forensics, A. Schroader & T. Cohen (2007)
[9] *Ibid*, Metropolitan Police Service – Digital Cyber and Communications Forensics Unit (2015).
[10] Interpol, Global Guidelines for Digital Forensic Laboratories, Interpol (2019)
[11] Europol, European Cybercrime Centre – Combating Crime in a digital age (2019)

9. In 2015, and recognising the absence of a legal definition, the Forensic Science Regulator for England and Wales provided a regulatory definition of digital forensics in the following terms:

'Digital forensics is the process by which information is extracted from data storage media (e.g. devices, remote storage and systems associated with computing, imaging, image comparison, video processing and enhancement [including CCTV], audio analysis, satellite navigation, communications), rendered into a useable form, processed and interpreted for the purpose of obtaining intelligence for use in investigations, or evidence for use in criminal proceedings.'[12]

(Forensic Science Regulator, Newsletter 26, October 2015)

10. From the above definition, it is apparent that several essential component parts must be present for an investigative process to constitute the application of 'digital forensic' techniques. Those key components are:

- Information must be extracted from digital storage media (as opposed to simply being viewed manually)
- The information is then rendered into a useable form
- The information is then processed and interpreted for the purpose of obtaining intelligence or evidence

11. Forensic Science processes, such as fingerprints or DNA testing naturally take precedence and may need to be conducted in order to establish a link between a mobile device and its owner or user. If the device is not handled properly during preservation and collection, physical evidence can be contaminated and rendered useless. Forensic Science processes on mobile devices should therefore be completed before digital forensic processes.[13]

PART 'A' – CURRENT ARRANGEMENTS

The current operating model in Scotland

12. Police Scotland now operates five interoperable Digital Forensic Hubs located in Glasgow, Edinburgh, Dundee, Inverness and Aberdeen. The purposes of these hubs are to facilitate the examination and extraction of a variety of digital devices in order to facilitate the collation of evidential material. The Edinburgh hub also hosts the Police Scotland Cyber Investigation Team. This design reflects a national service providing high-end specialist capability to all regions of Scotland. Accessibility and equity of service to the public is at the

[12] Forensic Science Regulator, Newsletter 26, October 2015: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/470526/FSR_Newsletter_26__October_2015.pdf

[13] The Scientific Working Group on Digital Evidence (2019) www.swgde.org

foundation of the culture and design of Police Scotland. The rationalisation of nine legacy sites to five Cyber Hubs created additional resilience by providing enhanced connectivity allowing for a standard, consistent approach which better meets demand.

13. The benefits of the current model by comparison with legacy arrangements have been self-assessed by Police Scotland as:

- Improved quality of digital forensic services as a result of rationalised, consistent and streamlined techniques, technology, processes and procedures
- Improved resilience and data security
- Increased effectiveness and efficiency
- Reduced organisational risk

14. On 20 January 2020, Police Scotland confirmed that it had commenced a phased roll-out of digital triage devices, also known as cyber kiosks. These devices had previously been tested in the live operational environment, however the operational roll out by Police Scotland was delayed by the Chief Constable following concerns raised by Members of the Scottish Parliament's Justice Sub-Committee in April 2019 about the legal basis under which such devices could be deployed.[14]

15. Following the Parliamentary concerns, Police Scotland undertook significant public consultation with external advisory and stakeholder groups and held a series of public engagement events during 2019. The Crown Office and Procurator Fiscal Service (COPFS), and independent Senior Counsel subsequently affirmed the legal basis for the use of cyber kiosks. 41 cyber kiosks have been procured and will be located at police stations across all policing divisions, and it is anticipated that all will be operational by the end of May 2020. Further information on cyber kiosks, including relevant policies, safeguards and the legal basis for their use has been published on the Police Scotland website.[15]

16. The primary reason why all UK police forces have introduced digital triage devices is because of the proliferation of electronic devices and media within society, the complexities of digital convergence and cloud computing, and related to this the consequence of investigative opportunities outstripping the current capacity of digital forensics analysts and investigators. In simple terms, the diversity of digital devices, complexity of hardware and software, virtual cloud-based storage, and sheer volume of data means that there is a national structural deficit in terms of the ability of policing to adequately resource electronic evidence opportunities.

> *'Increases in the involvement of digital devices in investigations and the ever-expanding capabilities of these devices means that demand on digital forensic examinations is higher than ever. Current limitations however, mean the devices of victims, witnesses and suspects can be taken for months at a time, even if it later*

[14] MSP's call for police 'cyber-kiosk' rollout to be paused, Scottish Parliament Justice Sub-Committee on Policing, 08 April 2019: https://www.parliament.scot/newsandmediacentre/111642.aspx
[15] Police Scotland cyber kiosks, policies, legal basis and impact assessments, 2020: https://www.scotland.police.uk/about-us/police-scotland/specialistcrime-division/cybercrime-investigations-digital-forensics/cyber-kiosks

transpires that there is no worthwhile evidence on them. By quickly identifying devices which do and do not contain evidence, we can minimise the intrusion on people's lives and provide a better service to the public'.

(Deputy Chief Constable Malcolm Graham, 14 January 2020)[16]

Current demand

17. Police Scotland Cybercrime Investigations and Digital Forensics have been working to ensure a consistency in terms of criteria for digital forensic examination. Any device seized lawfully by the police under common law, statute law, under warrant, or with consent may be considered for examination. The main reasons for the examination of digital devices fall under the following categories:

- Criminal investigations
- Death Enquiry
- Missing Persons Enquiries
- National Security
- On instruction from the Procurator Fiscal via Standard Fiscal Instruction (SFI)

18. Examinations will be conducted when:

- There is insufficient evidence to proceed to charge a person for a crime under investigation, and where there is a reasonable inference that a digital device may contain evidence of significance
- In the interests of National Security
- There is an urgency to examine devices that may prevent harm or risk, or there is a threat to life
- A Standard Fiscal Instruction (SFI) has been received by the Enquiry Officer or Senior Investigating Officer (SIO) from COPFS

19. Police Scotland, in common with most UK police forces are currently unable to meet the forensic demand in relation to digital investigations and more investment (fiscal, human, training and skills) is required in the digital space. Whilst the roll out of cyber kiosks offers the potential to reduce backlogs significantly, it is currently too early to offer a view on the extent to which those benefits will be realised.

20. In February 2020, data provided by Police Scotland suggests that there was a backlog of around 1200 outstanding cases solely in relation to telephones and computers awaiting digital forensic analysis. The overwhelming majority of forensic demand relates to mobile telephones which account for almost 90% of mobile devices, with around 25% of all demand pertaining to Standard Fiscal Instructions (SFI). In its Strategic review of Police Scotland's response to online child sexual abuse published in February 2020, HMICS made a specific recommendation (Recommendation No 9) that Police Scotland should work with COPFS to establish a pragmatic and realistic

[16] *Ibid,* Police Scotland website entry on cyber kiosks

approach to digital forensic examination requests.[17] The Police Scotland data showing outstanding examinations in February 2020, is illustrated by the following bar graph:

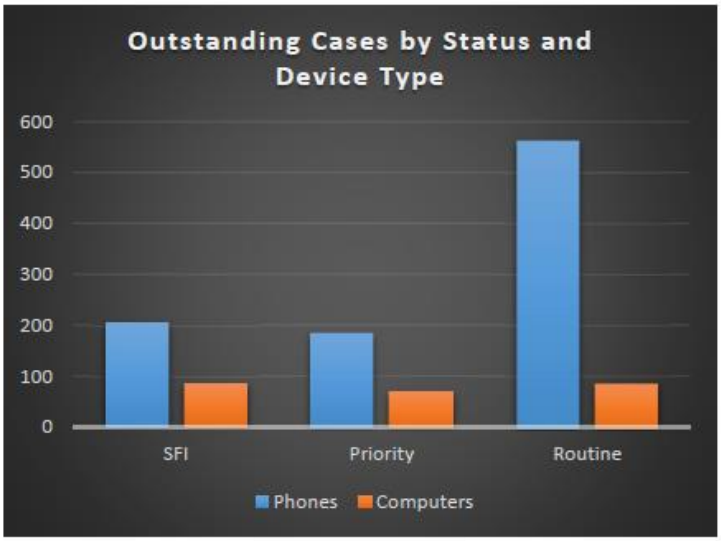


Figure No 1: Outstanding digital forensic cases phones and computers February 2020

21. One month earlier, in January 2020, and in response to a Freedom of Information (FOI) request, it was publicly reported that Police Scotland had a total backlog of 2553 items awaiting digital forensic analysis during the last 6 months of 2019.[18] This analysis reinforces the point made by DCC Malcolm Graham that seized devices are often queued awaiting digital examination for lengthy periods due to demand outstripping the capacity of the Digital Forensic Gateways and Hubs. The FOI response from Police Scotland included a detailed breakdown of all digital media examination requests as follows:

[17] Strategic Review of Police Scotland's response to online child sexual abuse, HMICS, February 2020: https://www.hmics.scot/news/police-scotland's-response-online-child-sexual-abuse-reviewed
[18] Response to FOI request by Police Scotland, published 26 January 2020, The Ferret: https://theferret.scot/police-scotland-backlog-digital-forensic-analysis/

Device type	Number
Camera	28
CCTV	2
CD / DVD disc	30
Computer tower	77
Games console	29
Hard drive	229
Laptop	219
Memory card	66
Other	31
Phone	1,483
Router	3
Sat Nav	2
Sim Card	34
Tablet	180
Tracking device	2
TV / TV devices	7
USB	131

Figure No 2: Data on outstanding digital forensic cases June to December 2019

(Source: Police Scotland FOI request, published in The Ferret, January 2020)

22. On 8 May 2019, the SPA presented a paper on digital triage devices to the Scottish Parliament Justice Sub-Committee on Policing. The paper revealed that in the calendar year 2017, Police Scotland had seized more than 40,000 mobile devices, and that 90% of mobile devices submitted for digital forensic examination were smartphones.[19] Therefore although there is a paucity of trend analysis data in relation to the exact number of digital forensic examinations carried out by Police Scotland in recent years, it may reasonably be inferred from the report to the Scottish Parliament and the various available statistics that current volumes may be in the region of 50,000 devices per annum. This means that the demand for digital forensics in Scotland by the second largest police force in

[19] SPA, Strategy Policy and Performance Committee report dated 8 May 2019.

the UK is directly comparable with similar digital volumes for investigations conducted by the Metropolitan Police, the largest UK force.

23. In a broader UK policing context, the proliferation of digital devices, the expansion of digital storage and the pace of change of digital technologies have made digital forensics the youngest, fastest growing and changing area of forensic science. Policing also seems to have a very limited understanding of the likely trajectory of digital demand, and given the fast-moving pace of technology, many UK policing practitioners feel that the service is always 'behind the curve'.[20]

24. In terms of long-term planning, stability and confidence is important to the long-range investment cycle and therefore there is a need for policing to keep pace with the anticipated path of likely changes in technological advancement. Significant financial investment will inevitably be required in the digital space to address these longer-term challenges. There is also a need for policing and the wider justice system in Scotland to better understand the potential trajectory of digital forensics in the years ahead. This will assist in determining optimum modes of transition to medium and long-term operating models, and better address the issues of capacity and capability, particularly in relation to in-sourcing models and decisions.

25. The department within Police Scotland that provides specialist digital support to all digital and cyber-related crime is Cybercrime Investigations and Digital Forensics which is located within the Specialist Crime Division (SCD), Organised Crime and Counter Terrorism Unit (OCCTU). At the time of writing, there are 68 digital forensic examiners across Police Scotland to support operational activity. 29 (43%) of these are police officers and 39 (57%) are police staff. These figures include the Cyber Investigations Team based in Edinburgh. Their role is to support the development of digital forensic strategies and prioritise the examination of digital devices. In addition, 410 local police officers throughout Scotland are trained in the operation of digital triage devices.

26. The Digital Forensic Gateway is the receiving facility for all examination request forms where triage and quality control functions are conducted. Gateway staff are co-located within the 5 Digital Forensic Hubs to provide a consistent process. Digital Forensic Examiners (DFE) receive training in a range of digital and cyber-crime disciplines. The training in the various available modules is delivered and accredited to UK Policing by the College of Policing and seeks to equip DFE's and investigators with core skills in data recovery and to undertake and investigate offences involving a high-tech element. Further information can be found on the College of Policing website.[21] In addition, some specialist training is outsourced by Police Scotland, and Police Scotland also uses software provided by external companies used by law enforcement and E-Discovery agencies.

[20] Forensics Review: Review of the provision of forensic science to the criminal justice system in England and Wales, Home Office: July 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/800447/Joint-review-of-forensics-provision-July-2018.pdf

[21] Digital and Cybercrime, College of Policing, 2020: https://www.college.police.uk/What-we-do/Learning/Professional-Training/digital-and-cyber-crime/Pages/Digital-and-cyber_crime.aspx

27. Forensics within the Cybercrime Unit functions ostensibly as a service unit. This means that they are tasked to conduct only one part of a criminal investigation. All work is done at the request of an Investigating or Reporting Officer, with the ownership and responsibility of reporting matters, including disclosure obligations, remaining solely with the local officer in charge of the case. For an examination to be undertaken, the local officer must complete and submit an electronic Cybercrime Examination Request Form (ERF). This document, which is fully auditable and disclosable, sets out the parameters of the request and provides details of the matter under investigation. Only work that has been subject to assessment and approved by the National Cybercrime Gateway Unit will be authorised for examination/analysis. This process ensures that a consistent process is applied in line with the Police Scotland document *'Digital Device Examination Principles'.*

28. This type of individual client service-based operating model results in some strategic gaps for Police Scotland in terms of holistic overview, high-end capacity and capability, and the capacity to provide expert witnesses in digital cases. It also means that there is no centralised or accredited quality control mechanisms in place in relation to the corporate delivery of digital forensics by Police Scotland as highlighted by HMICS recommendation in 2017. This will be discussed further in this report when turning to consider accreditation and quality management systems.

29. In the recent HMICS Strategic review of Police Scotland's response to online child sexual abuse published in February 2020, HM Chief Inspector of Constabulary in Scotland explores digital forensics case management and technology/skills maintenance and notes problems with demand management and skills shortages. However, HMICS notes (paragraph 174) that Police Scotland has recently established a capacity and capability expansion programme around Cybercrime and Technical Surveillance through a CTSP Programme Board, CTSP Steering Group and the Scottish Sensitive Equities Board[22] as part of a programme of a wider programme of improvement.

30. In order to understand current and future demand, it is also necessary to reflect on the complexities of digital investigations and what this means in terms of the time and resources taken in a single investigation. It is also common for individual users to access numerous digital devices and physical and cloud-based storage mediums. The consequence of this is that both the volume and location of data presents numerous investigative challenges. In addition, criminals will use a manner of methods to obfuscate their data, identity and location. Furthermore, with advances in consumer-level encryption, accessing data without consent is sometimes not achievable as highlighted by the well-known FBI vs Apple encryption dispute in 2016.[23] The following case studies from Scotland illustrate this complexity:

[22] The CTSP Programme Board and the Scottish Sensitive Equities Board is chaired by the ACC Organised Crime, Counter Terrorism and Intelligence and looks at covert capability. The Steering Group is chaired by the Detective Superintendent, Cyber Investigations, Digital Forensics and CTSP.

[23] The Apple- FBI case, New York Times, 2016: https://www.nytimes.com/news-event/apple-fbi-case

Case Study No 1:
In March 2019, one of Scotland's most prolific online groomers was jailed for 12 years after targeting scores of young girls in Edinburgh for sex attacks. Gavin Scoular (24) identified his victims aged 12 to 17 years through digital platforms such as Facebook, Snapchat and Skype. He was found guilty of numerous child rapes and passing sentence, Lord Summers spoke of 'the industrial scale of the offending'. A case such as this includes a significant digital component to the overall investigation necessitating thousands of hours of digital review, recovery, cataloguing and assessing.[24]

Case Study No 2:
In March 2020, one of Scotland's most prolific paedophiles Robert Wilkinson Brown (51) appeared at the High Court in Glasgow admitting offences of possessing indecent images of children. Police had found more than 75,159 images of child sexual exploitation during digital forensic examination some of which were on memory sticks and a USB. The court heard from Police Scotland that two IP addresses had been used to access indecent images of children. 145 hours of video footage was also recovered from a single device depicting male children. This case study also demonstrates the sheer volume of data within a single investigation and the problem of data overload which takes thousands of hours to recover, catalogue and assess as part of the overall investigation.[25]

Future demand

31 Each year, Europol's European Cybercrime Centre (EC3) publishes the Internet Organised Crime Threat Assessment (IOCTA), its flagship strategic report on key findings and emerging threats in cybercrime. These strategic threats impact on governments, businesses and citizens and the conclusion of both Europol and Interpol is that both digital crime and digital evidential opportunities will grow exponentially.[26]

32. IOCTA 2019, highlights that the ability of law enforcement agencies to conduct criminal investigations is an increasing challenge. This is as a result of various factors including the enhanced use of encryption which criminals use to obfuscate their location and identity, as well as an exponential growth in the use of the dark-web and cryptocurrencies.

[24] Man who groomed and raped girls in Edinburgh jailed, BBC, March 2019: https://www.bbc.com/news/uk-scotland-edinburgh-east-fife-47415703
[25] Scots paedo's huge stash of child images contained 'some of the worst' police had ever seen, Daily Record, March 2020: https://www.dailyrecord.co.uk/news/scottish-news/scots-peados-huge-stash-child-21680940
[26] IOCTA 2019, Europol EC3 Cybercrime Centre: https://www.europol.europa.eu/iocta-report

33. At the same time, there is also the ever-increasing challenge of data overload, particularly in areas such as Child Sexual Exploitation (CSE). The amount of Child Sexual Exploitation Material (CSEM) detected online by law enforcement and the private sector continues to increase. This increase puts a considerable strain on law enforcement resources and similarly requires a long-term planning response to ensure that the volume of data does not impede law enforcement authorities' responsibility to conduct criminal investigations into CSEM.

34. Self-generated explicit material (SGEM) and 'Sexting' is another significant growth area in Scotland and internationally, driven by a growing number of children with unregulated access to high-quality smartphones. On top of this growing access, a lack of awareness of the risks on the part of children further exacerbates the problem.

35. In the UK, the National Crime Agency (NCA), National Strategic Assessment of Serious and Organised Crime 2019 includes several digital threats to UK law enforcement.[27] The NCA note that advancing technology gives offenders new tools to commit and hide their crimes. Today's criminals can sell drugs, share indecent images of children, or hack into national infrastructure from anywhere in the world, communicating covertly through encrypted services and moving illicit finances at speed. Child sexual abuse and exploitation (CSAE) remains a high-volume offence, with recorded instances increasing across the UK.

36. Police Scotland is aware of the structural and financial deficit in terms of the ability of policing to adequately resource electronic evidence opportunities, and that all available information and intelligence points to a continued growth in demand for greater digital forensic capacity and capability in the years ahead. This will require new approaches and a journey of transition including the development of options to address current, medium and longer-term demand.

37. In 2017, Police Scotland published its Procurement Strategy 2017-2020.[28] The strategy document explained that Police Scotland had commenced two major programmes of transformation: Cybercrime Capability Programme (CCP) and the Technical Surveillance for the 21st Century Programme (TS21C). The aim of both programmes at this juncture was to review and transform capability and capacity across the three related functions of cybercrime, digital forensics and technical surveillance.

38. More recently, Police Scotland has now combined these programmes into a single unified Cybercrime and Technical Surveillance Programme (CTSP). This is to ensure a more holistic overview and greater executive focus. As part of these developments, Scottish Government project funding has been secured to employ three additional dedicated analysts to Cybercrime Intelligence and Digital Forensics. However, the challenges for Police Scotland are significant, as there are also resourcing and structural challenges in many

[27] National Crime Agency (NCA), National Strategic Assessment of Serious and Organised Crime, 2019: https://nationalcrimeagency.gov.uk/who-we-are/publications/296-national-strategic-assessment-of-serious-organised-crime-2019/file

[28] Police Scotland, Procurement Strategy 2017-2020: https://www.scotland.police.uk/assets/pdf/138327/327595/procurement-strategy-2017-2020

related digital disciplines such as the Internet Investigation Unit (IIU) and the Telecommunications Investigation Unit (TIU). These issues were highlighted in the HMICS Strategic review of Police Scotland's response to online child sexual abuse published on 26 February 2020. All of this points to the need for greater investment (fiscal, human, training, skills) in the digital space by Police Scotland.

Scottish Government Digital Strategy for Scotland

39. In March 2017, Scottish Government published a Digital Strategy for Scotland: Realising Scotland's full potential in a digital world.[29] The strategy sets out the development and implications of new and emergent technologies and digital platforms such as the internet of things, cloud computing, sensors, artificial intelligence and machine learning. It also demands that we challenge old ways of thinking about public services and the organisations that deliver them.

40. Realising Scotland's full potential in a digital world is a strategy for Scotland, not just the Scottish Government. It recognises the profound challenges that digital poses for the nature of work, for society, for our public services and for the economy. It looks to create a culture and environment of partnership and collective action and to ensure public safety and security. As recognised in the Ministerial Foreword, '…digital disrupts traditional jobs and industries, puts new pressures on our right to privacy and has the potential to create new forms of social exclusion. It generates new opportunities for criminal exploitation and raises serious questions for national and international security'.

41. In March 2018 the Scottish Government published a desk-based review entitled 'Cyber-Crime in Scotland: A review of the Evidence'.[30] The purpose of the review was to better understand how cyber-technology and digital was impacting on crime in Scotland. This against the context of several key strategies highlighting the challenges presented by cyber-crime. This included the Justice Vision and Priorities, setting out the Scottish Government's plan for a just, safe and resilient Scotland.[31] Police Scotland and the SPA 2026 strategies, the Scottish Government's Serious and Organised Crime Strategy,[32] and Safe, Secure and Prosperous: A Cyber Resilience Strategy for Scotland.[33] The review highlighted the growth in the use of the internet and digital technologies and the potential for criminals and others to exploit this growth.

---

[29] Realising Scotland's full potential in a digital world: A Digital Strategy for Scotland, Scottish Government, 2017: https://www.gov.scot/publications/realising-scotlands-full-potential-digital-world-digital-strategy-scotland/

[30] Cyber-crime in Scotland: A Review of the Evidence, Scottish Government Crime and Justice Social Research, March 2018: https://www.gov.scot/publications/cyber-crime-scotland-review-evidence/

[31] Justice in Scotland: Vision and Priorities, Scottish Government, July 2017: https://www.gov.scot/publications/justice-scotland-vision-priorities/

[32] Scottish Government Serious Organised Crime Strategy, June 2015: https://www.gov.scot/publications/scotlands-serious-organised-crime-strategy/

[33] Safe, Secure and Prosperous: A Cyber Resilience Strategy for Scotland, Scottish Government, November 2015: https://www.gov.scot/publications/safe-secure-prosperous-cyber-resilience-strategy-scotland/

42. In 2019, the Scottish Government launched a procurement process for a new Digital Evidence Sharing Capability (DESC), which will allow users such as police officers, prosecutors, court staff and defence agents to digitally access evidence. The initiative has the potential to improve effectiveness and efficiency within the criminal justice process as well as enabling earlier consideration and disclosure of evidence.[34]

> *'…Reducing delays is just one of the benefits of this project, which will make evidence sharing more cost effective and provide the groundwork for further modernisation of the criminal process'.*
>
> (Humza Yousaf, Cabinet Secretary for Justice: 29 September 2019)

43. Therefore, existing Scottish Government strategy recognises that further investment in the digital space offers the potential to challenge old ways of thinking and to further enhance the effectiveness of the justice process through a range of digital data and evidence sharing initiatives. As part of this, the Scottish Government is in the process of establishing an Emerging Technologies Independent Advisory Group. This follows on from a warning by MSPs that some policing technologies emerging in England and Wales such as live facial recognition would be a radical departure from the current practice of policing by consent if ever considered for Scotland.[35]

Existing governance of Forensic Science and digital forensics

Forensic Science services delivered by SPA Forensic Service

44. Forensic Science services in Scotland is provided to Police Scotland by SPA Forensic Service to ensure differentiation or a sterile corridor to delineate the police investigation from the scientific investigation. The national Forensic Services model in Scotland is internationally acclaimed and places quality and accreditation at the heart of everything. The sterile corridor principle, through differentiation, also exists to exonerate the innocent.

45. Most of the work of SPA Forensic Service has been accredited to deliver scientific and forensic services by the United Kingdom Accreditation Service (UKAS) for more than 20 years. Third-party assessment by UKAS accreditation offers confidence that forensic activities are carried out impartially and competently. Compliance with the relevant international ISO Standard infers the highest standards of personal conduct, and organisational compliance with such quality standards. Accreditation, quality assurance systems, and individual assessment of competence also enables SPA Forensic Service to provide an 'expert witness' service to the courts. This means a person whose level of

[34] Improving Digital Evidence Sharing, DESC Programme, Scottish Government, 2019: https://www.gov.scot/news/improving-digital-evidence-sharing/
[35] Police urged to abandon facial recognition scans, The Times, 20 May 2020.

specialised knowledge and accredited skill or expertise in a discipline (for example ballistics) qualifies them to present their opinion and interpretation about the facts of a case during legal proceedings.

46. SPA Forensic Service collaborates effectively with the Forensic Science Regulator (FSR) for England and Wales, and in turn, the FSR collaborates with the devolved authorities in Scotland and Northern Ireland who have expressed a willingness to be partners in the setting of quality standards which will be adopted within the devolved justice systems. This UK cooperation is essential given that many of the UK forensic and biometric databases in use are provided and maintained by the Home Office, for example the National DNA Database (NDNAD) which includes data from the Scottish DNA Database (SDNAD) and IDENT1 the single national automated fingerprint system that provides biometric services to all UK police forces and law enforcement agencies.

47. The crime scene to court model operated by SPA Forensic Service is illustrated on the next page of this report by the following extract from the Forensic 2026 Strategy:[36]

[36] SPA Forensics 2026 Strategy, Scientific Excellence for Safer Communities: http://www.spa.police.uk/assets/126884/441011/441165/457127/item7.1i

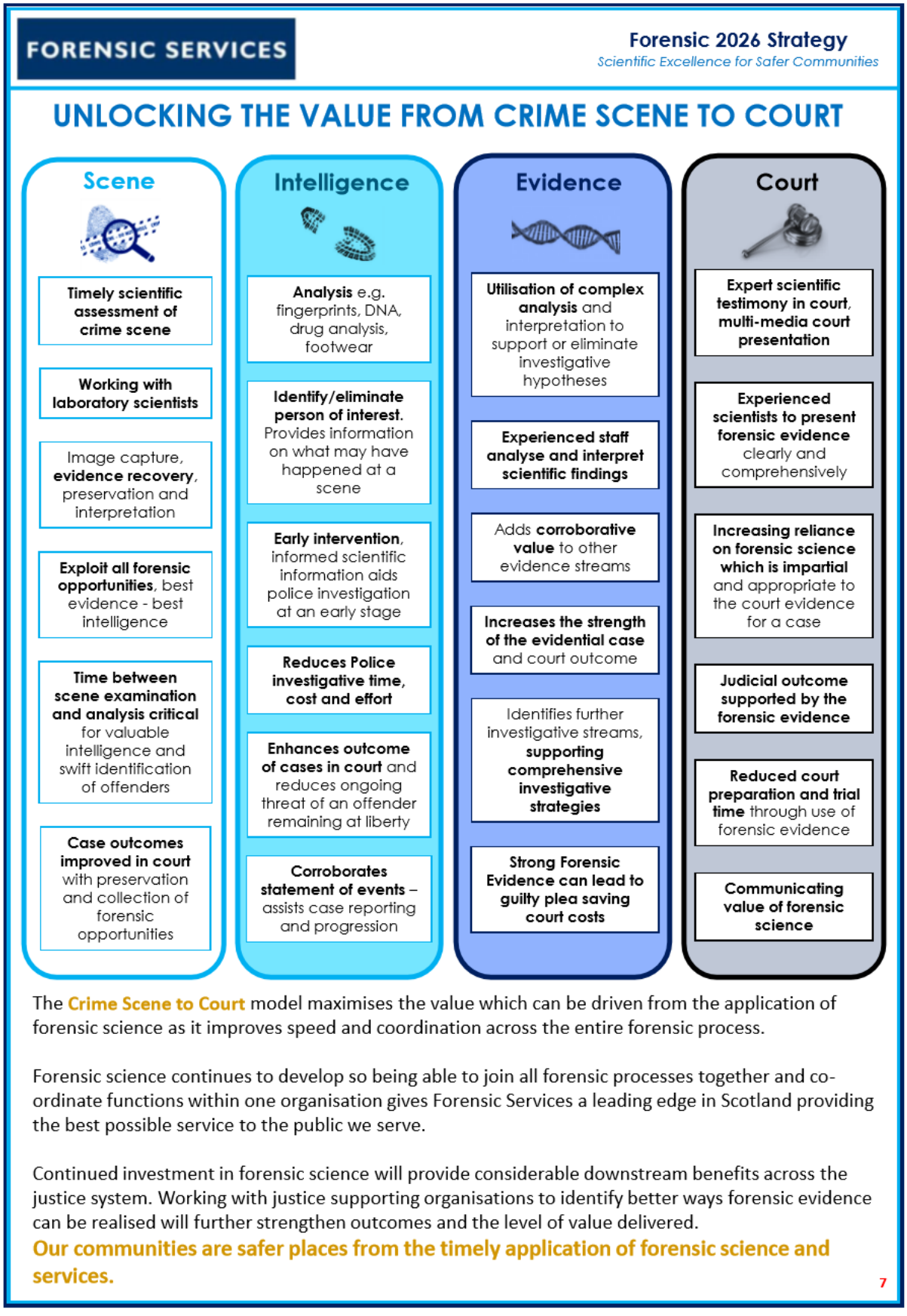


Figure No 3: The Crime Scene to Court Model (Source: SPA Forensic Strategy to 2026)

Digital Forensics delivered by Police Scotland

48. Unlike Forensic Science, the delivery of digital forensics in Scotland does not sit with scientific staff within SPA Forensic Service but instead sits as an operational function of Police Scotland. Executive responsibility rests within the business areas managed by the Deputy Chief Constable Crime and Operations, with digital forensics and cybercrime falling within the operational portfolio of the Assistant Chief Constable Organised Crime, Counter Terrorism and Intelligence.

49. Police Scotland has conducted an impact assessment of current and future demand in relation to digital forensics.[37] The Police Scotland impact assessment notes the exponential growth of digital devices within society and the requirements for policing to keep pace with this change. The impact assessment concludes that transformation and modernisation of policing practices and capabilities is necessary.

50. The ability of Police Scotland to provide an immediate and consistent digital forensics service is critical to the service as it supports the delivery of all four Policing Priorities from the Annual Police Plan 2019/20:[38]

- Protecting vulnerable people
- Tackling cyber related crime
- Working with communities
- Support for operational policing

51. The Police Scotland impact assessment notes that the use of digital forensics techniques affords policing access to highly sensitive personal data and notes the obvious tension between the needs of law enforcement, the rights of private individuals, and the broader privacy, human-rights and ethical considerations that arise. One such issue is the significant problem of collateral intrusion, as examination of digital devices often affords the police access to highly-sensitive personal information about associates unconnected with the matters under investigation, including biometric data such as photographs and access to private communications that have been exchanged on encrypted platforms.

52. Recognising such challenges, Data Ethics is an area of growing importance across UK Policing and is under active discussion within the National Police Chiefs' Council (NPCC). Police Scotland are part of this work and are also in the process of establishing a data ethics governance framework. This is to assist Police Scotland in complying with data protection legislation and privacy regulations, to ensure fair and reasonable data use, and to maximise the use of data for public good and ensure the continued legitimacy of policing.

53. Following engagement with the Scottish Parliament Justice Sub-Committee on Policing on the topic of cyber-kiosks, Police Scotland has sought to provide greater

[37] Restricted briefing paper to ACC Organised Crime, Counter Terrorism and Intelligence, February 2020 shared with DFWG.
[38] Police Scotland Annual Police Plan 2019-2020: Serving a Changing Scotland: https://www.scotland.police.uk/assets/pdf/138327/150739/annual-police-plan-2019-20?view=Standard

transparency in relation to digital forensics and have produced and published a suite of accessible information documents. This includes a short video summary explaining what cyber-kiosks are, 5 separate documents on the technical examination process, the legal basis and opinion on the lawfulness of cyber-kiosks, and data protection and equality and human-rights impact assessments. It should be noted however that this public information is solely in relation to digital triage devices and not on the actual digital forensic procedures and process that take place within the 5 Cyber Hubs.

54. Unlike the forensic science services provided by the SPA Forensic Service, Police Scotland has not yet sought to independently accredit any aspects of the digital forensic services that it operates. This despite the recommendation from HMICS in 2017 that Police Scotland should consider quality accreditation for digital forensics in line with the Forensic Science Regulator (FSR) recommendations, the Home Office Forensic Strategy for England and Wales, and wider good practice in order to support effective public performance reporting and assurance.[39]

55. In England and Wales, the Forensic Science Regulator requires all policing providers of digital forensics to be accredited through UKAS to the relevant international quality standard to ensure that forensic services are carried out competently and impartially. In addition, the FSR has instructed that the absence of accreditation by a force in a particular discipline must be disclosed in relevant criminal proceedings so that prosecutors and the defence are aware that the reliability and validity of the processes and procedures used to retrieve digital evidence have not been independently quality assured.

56. For Scotland which does not have its own FSR, this means that different approaches are currently being taken to the accreditation of different forensic services. On one hand forensic science services as delivered by the SPA Forensic Service are accredited by UKAS to defined international quality standards. On the other, the newer yet arguably far more intrusive area of digital forensics is not. This carries significant reputational risk for Police Scotland, particularly given the move to accreditation of digital forensics in England and Wales, the endorsement of ISO accreditation standards for digital forensics laboratories internationally by Interpol,[40] and the 2017 recommendation from HMICS.

57. Following the 2017 recommendation by HMICS that Police Scotland should consider accreditation of digital forensics, an internal police Scotland paper recommended the development and establishment of a quality management system around digital forensics and the appointment of a quality manager to begin the journey of transition towards accreditation. In paragraph 176 of the 2020 HMICS Strategic review of Police Scotland's response to online child sexual abuse, it was stated that Police Scotland has failed to make any progress on this. However, Police Scotland has since clarified that in 2019 a Data Quality Assurance Manager for Cybercrime and Digital Forensics was appointed in the recognition of the need to develop a quality assurance and management framework. The DFWG

[39] It should be noted that the 2017 HMICS recommendation arose from an inspection of the delivery of Forensic Services to Police Scotland by the SPA, and not a specific inspection of digital forensics
[40] Interpol, Global Guidelines for Digital Forensic Laboratories, May 2019:

welcomes this, however, supports the general finding by HMICS that further progress on quality management and accreditation is required to address questions that otherwise arise in relation to the perceived validity and reliability of digital evidence in Scotland.

58. The following figure highlights some of the publications discussed that are of direct relevance to contemporary debates on the importance of accrediting digital forensics:

Figure No: 4 Scottish Parliament, HMICS and Interpol reports pertinent to Digital Forensics

PART 'B' – FUTURE ARRANGEMENTS

Future delivery and governance – Options appraisal

59. In accordance with the published terms of reference for the DFWG, one of the first tasks was to conduct and options appraisal to review current and alternative service delivery models for digital forensics in Scotland and analysing their relative costs and benefits. This was developed following an initial literature review exploring alternative domestic and international options,[41] and in accordance with the best practice guidance on option appraisal as contained in the HM Treasury, Green Book, 2018.[42]

60. Before turning to consider the various options, it should be noted that there are many reasons why crime-scene forensic science disciplines have fallen primarily to 'scientists' as many of the scientific techniques deployed in such forensics necessitate particular scientific skills, qualifications and accreditation in the sciences of biology and chemistry in particular.

61. By contrast, digital forensics is concerned with the recovery of electronic evidence and data from devices and networks and relies less on 'pure science' and more on technical ICT skills around data recovery and analysis. This explains why digital forensics in UK policing has traditionally been within the service, as the work of the detectives and data analysts (although sometimes forensic in nature) has a significant intelligence gathering function, for example in the identification of associates and criminal networks, as well as that of an

[41] Digital Forensics Literature Review for DFWG, prepared by Dr Brian Plastow, October 2019 (unpublished).
[42] HM Treasury Green Book, 2018: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/685903/The_Green_Book.pdf

evidential nature. Digital forensics are also a feature of some high-paced police operations where 'real-time' 24/7 x 365 information is required on time critical matters, and on broader matters of UK national security.

62. Therefore, although both disciplines share a common 'forensic' nomenclature, it would be too simplistic an argument to conflate both as necessitating an identical operating model without properly and fully exploring the three related themes of desirability, viability and feasibility. This definitional conundrum is compounded by the absence of a legal definition of 'Forensic Services' within the Police and Fire Reform (Scotland) Act 2012.[43]

63. Early discussion within the DFWG included consideration of whether all forensic techniques, including digital could/should be delivered by SPA Forensic Service, and what other options existed including the status quo. Following consideration of potential operating models, the following shortlist of options was considered by the DFWG and is summarised as follows:

Option No	Delivery Model	Cost/Benefit Analysis
1	Transfer digital forensics from Police Scotland to SPA Forensic Service to provide clear separation between the police and scientific investigations in line with the 'sterile corridor' principle.	Costs would outweigh benefits having regard to strategic, economic, management and financial dimensions as 42% of digital examiners are serving police officers. Transfer would require at least 29 new police staff. Specialist recruitment would be problematic.
2	Digital Forensics remains with Police Scotland (Do nothing option).	Best fit in absence of clear case for strategic change. Aligns with needs of Police Scotland and is only option to meet the HM Treasury cost/benefit analysis test.
3	Outsource digital forensics to third-party provider	Would result in loss of control of quality and raise resilience concerns. Comparison with Metropolitan Police £8 million outsource.[44]
4	Create new National Forensics Body (NDPB) as per the Netherlands Forensic Institute Model.[45]	Costs would outweigh benefits having regard to strategic, economic, management and financial dimensions including the needs of operational policing.

Figure No 5: DFWG Options Appraisal Summary

[43] Police and Fire Reform (Scotland) Act 2012, paragraph 31
[44] Metropolitan Police outsource Digital Forensics in seven year deal worth £8 million: ComputerWeekly.com: https://www.computerweekly.com/news/450422403/Met-Police-signs-8m-digital-forensics-deal
[45] Netherlands Forensic Institute: https://www.forensicinstitute.nl/

64. In relation to service delivery models, and following extensive consultation, the conclusion of the DFWG is that there is no current robust business case for an alternative operating model in Scotland, and to do otherwise would require significant financial investment at a time when police finances are already under considerable strain. Therefore, the delivery of digital forensics in Scotland should remain with Police Scotland under the operational responsibilities and internal governance arrangements of the Chief Constable. This decision does not however preclude the future alignment of forensic laboratory work should benefits realisation parameters change as a result of a wider review of all forensic service provision in Scotland. As previously highlighted by Audit Scotland, any structural changes around digital, data and ICT require financial sustainability, and in the view of the DFWG the most financially sustainable option is for digital forensics to remain with Police Scotland.[46]

65. As discussed in the earlier future demand section of this report, Police Scotland has now established a Cybercrime and Technical Surveillance Programme (CTSP). CTSP is a transformation programme for Cybercrime Investigations, Digital Forensics and Technical Surveillance ensuring specialist and niche capability to support Police Scotland in terms of investigation and intelligence activity. The CTSP Programme Vision is:

> *'Keeping people safe in a digital world; continuously improving and evolving our services to maintain excellence and keep operations at pace with technology and criminal tactics'.*
>
> (Police Scotland CTSP Programme Vision, 2020)

66. The CTSP has 4 key themes:

Digital Knowledge & Skills – Digital and technological investigative capability will be enhanced by building and upskilling a workforce with the skills and knowledge to ensure that we are appropriately equipped to provide investigative services when tackling any crime with a digital, technological, cybercrime or surveillance facet.

Digital Infrastructure – We will establish an agile, efficient, resilient and secure technical infrastructure that will enable Cybercrime and Technical Surveillance to capitalise on advanced and emerging technologies increasing asset capability, digital product quality and facilitate more intelligent and effective data analysis.

Digital Investigative Capability & Capacity – We will invest and build our investigative capability. Enhanced and meaningful investigative reporting capability, which will lead to effective decision making across the organisation by providing enhanced insight into current demand and opportunities to exploit the criminal digital footprint.

[46] Audit Scotland, the 2018 Audit of the SPA Section 22 Report: https://www.audit-scotland.gov.uk/report/the-201819-audit-of-the-scottish-police-authority

Digital Innovation – Will identify opportunities to work in partnership with International and UK law enforcement, government agencies, academic institutions and key market leaders to develop the perpetual innovation of technologies, assets, tactics and techniques.

67. These developments within Police Scotland will lead to the development of a new Target Operating Model (TOM) which will have personnel implications regarding re-structure, recruitment, knowledge and skills opportunities. At the time of writing, work is ongoing within Police Scotland to finalise budget allocation for Programmes and Departments within Police Scotland for 2020/21.

68. Given the obvious inter-relationship between cybercrime, digital forensics and technical surveillance, it is the conclusion of the DFWG that the operational delivery of digital forensics should remain with Police Scotland under the operational responsibilities and internal governance arrangements of the Chief Constable.

Recommendation 1
The delivery of digital forensics should remain with Police Scotland under the operational responsibilities and internal governance arrangements of the Chief Constable.

69. In Scotland, the SPA Forensic Services Committee (FSC) provides external governance and assurance over forensic science. The purpose of the FSC is to '…provide oversight, scrutiny and assurance to the Board on the delivery of Forensic Services to the Police Service, Police Investigations and Review Commissioner (PIRC) and the Lord Advocate and Procurators Fiscal as set out in Section 31 of the Police and Fire Reform (Scotland) Act 2012. The committee will provide advice and seek assurance on the delivery of Forensic Services by providing constructive challenge and contributing to planning and future development of Forensic Services'.[47]

70. Because digital forensics are delivered by Police Scotland rather than SPA Forensic Service, this means that digital forensics had not previously been within the published terms of reference for the FSC. The Authority has established a number of committees to undertake specific functions, to carry out more detailed scrutiny work in particular areas and to assist and advise it in relation to the performance of its functions, thereby enabling the Board to maintain a focus on major issues facing the organisation.

71. However, given the recent establishment of the Cybercrime and Technical Surveillance Programme as a major programme of change encompassing digital forensics, and the inter-relationship between forensic science and digital forensics there is a need for the SPA Board to consider how best to discharge and balance its responsibilities in terms of supporting policing and holding the service to account. The DFWG therefore recommends that the SPA Board should agree the most appropriate Committee(s) to have oversight,

[47] SPA Corporate Governance Framework, 2018: http://www.spa.police.uk/assets/128635/293617/487394/488996

scrutiny, and assurance over Police Scotland's Cybercrime and Technical Surveillance Programme (CTSP).

Recommendation 2
The SPA Board should agree the appropriate Committee(s) to have oversight, scrutiny, and assurance over digital forensics, and the areas covered by the Police Scotland Cybercrime and Technical Surveillance Programme (CTSP).

72. More broadly, and in the absence of a Forensic Science Regulator in Scotland, digital forensics and the CTSP may be areas worthy of inclusion as part of a future thematic scrutiny programme by HMICS following determination of, and transition to, a new target operating model. In addition, the SPA FSC will be aware that the Bill to introduce a Scottish Biometrics Commissioner was passed into law by the Scottish Parliament on 10 March 2020. This, together with an associated Code of Practice on the acquisition, use, retention and disposal of biometric data held for policing purposes will strengthen existing oversight arrangements. Given the ability of digital forensics techniques to overcome certain biometric access controls on digital devices, and to capture and process biometric data held therein, there will be a requirement for digital forensics to adhere to any Codes of Practice subsequently developed by the Biometrics Commissioner for Scotland. This will provide an additional layer of external governance and assurance to maintain public confidence in policing in Scotland.

Accreditation and quality management

Accreditation of Forensic Science

73. In 2016, the Home Office produced a Forensic Science Strategy setting out a national approach to forensic science delivery in the criminal justice system for England and Wales.[48] The strategy seeks to deliver an approach that reinforces the legitimacy of forensic science delivery to the criminal justice system through consistent quality management across police forces, including a clearer statutory role for the Forensic Science Regulator in England and Wales. Scotland and Northern Ireland have their own criminal justice systems but follow the FSR's standards for forensic science.[49]

74. The strategy highlights that forensic science in the UK is delivered to a high standard that is acknowledged globally. However, these standards have only been achieved by embracing the significant learning from high profile cases in the past where forensic science has failed, and where as a consequence, the legitimacy, credibility and validity of forensic

[48] Forensic Science Strategy: A national approach to forensic science delivery in the criminal justice system, Home Office, 2016: https://www.gov.uk/government/publications/forensic-science-strategy
[49] *Ibid*, quality management systems, paragraph 39.

investigations, and the reputation of policing, has been seriously undermined in terms of public confidence and trust.

75. The Home Office Forensic Science Strategy cites by way of example the acquittal of the "Birmingham Six" in 1991, who were jailed for the Birmingham pub bombings of November 1974. The case against the Birmingham Six collapsed when fresh evidence caused the Court of Appeal to cast doubt on a key piece of forensic evidence used at the original trial to secure the convictions. This, and similar cases, have led to rigorous quality standards being put in place to determine a common and consistent approach on how forensic science is applied. These standards are determined by the Forensic Science Regulator and published in the FSR Codes of Practice and Conduct. All commercial and police providers are expected to conform to the standards.

76. In Scotland, there is also significant past learning to be taken from the absence of quality management systems and safeguards within specific forensic science disciplines, and the consequence in terms of serious miscarriages of justice and damage to public confidence in policing. For example, in 2011 the publication of the findings of the Scottish Fingerprint Inquiry led by Sir Anthony Campbell into the Shirley McKie fingerprint case exposed how failings in systems and processes within the former Scottish Criminal Records Office (SCRO), led to the former police detective being wrongly arrested, charged, and dismissed by the then Strathclyde Police, before ultimately being acquitted in 1999.[50]

77. The Fingerprint Inquiry was a public inquiry set up by Scottish Government ministers under the Inquiries Act 2005 to look at the steps which had been taken to verify the fingerprints associated with the case of *HM Advocate v McKie* in 1999. The Inquiry terms of reference was to determine the consequences of steps taken, and to report on findings of fact and make recommendation. The Scottish Fingerprint Inquiry made no less than 86 recommendations for future action and improvement. It was the catalyst for significant improvements in quality management systems around fingerprint comparison, including formal accreditation of methods and processes.

78. In 2016, and 5 years on from the findings of the Scottish Fingerprint Inquiry, SPA Forensic Service became the first large scale provider in the UK to receive accreditation from the United Kingdom Accreditation Service (UKAS) for its fingerprint comparison activities. The award of ISO/IEC 17025 accreditation placed the fingerprint service on the same international standard as other science-based elements of SPA Forensic Service. Such accreditation to a recognised international quality standard, demonstrates that systems of working and evidence gathering procedures have been externally assessed against stringent standards and have been deemed competent, robust, consistent and fit for purpose in carrying out and reporting on fingerprint examinations which are impartial, objective and fit for purpose.[51]

[50] The Fingerprint Inquiry Scotland: Scottish Government, 2011 (Archived).
[51] Fingerprint Service in Scotland leading the way in the UK, December 2016: http://www.spa.police.uk/news/437866/373775/

79. In Scotland, there is no such externally validated, or accredited mechanisms in place in relation to the delivery of digital forensics by Police Scotland as highlighted by HMICS recommendation in 2017. Whilst Police Scotland believes it has strong internal governance arrangements in place, these have not been independently validated, and it is the opinion of the DFWG that there needs to be independently assessed quality assurance arrangements to reflect similar standards in other forensic disciplines. This is necessary to ensure and confirm the integrity of digital forensic investigation processes which culminate in reports to COPFS, and similarly the work of digital forensic practitioners. It should be emphasised that no challenges to the veracity of digital evidence have emerged through the Scottish courts, but Police Scotland are alert to the challenges.

80. Such systems and procedures should include externally validated mechanisms to identify and record mistakes or bias, to confirm the continued validity and reliability of standard operating procedures and protocols, and to ensure that best practice and the rules of disclosure are being followed. Independent oversight and assurance are also considered necessary to maintain public confidence and trust in an area where both digital technologies, and consequentially evidential opportunities, are advancing at pace.

81. Of course, no system of accreditation can eliminate the possibility of an individual mistake being made, whether intentional or in error. However, without such external validation of the systematic approach being taken to digital forensics by Police Scotland, the DFWG concludes that evidence obtained through digital forensics techniques cannot be considered as having equivalence with the validity, reliability and accuracy of evidence obtained through externally accredited forensic techniques. This was a view strongly supported during our consultation and engagement with stakeholders. The potential accreditation of digital forensics will be explored further in the following paragraph: however, it is worth reflecting that the process of organisational learning is iterative and not a static or one-time event.

> ***'…Those who cannot remember the past are condemned to repeat it'***
>
> (George Santayana, philosopher 1863 to 1952)

Accreditation of digital forensics

82. For forensic science to contribute effectively to the criminal justice system the science must be trustworthy. Two key components of this are quality management standards and training.[52] Since October 2017, the Forensic Science Regulator's (FSR) Code of Practice stipulates that all providers of Digital Forensic services to the criminal justice system in England and Wales must be accredited to ISO-17025, and that failure to achieve accreditation must be disclosed to the courts when digital evidence is presented by a non-

[52] House of Lords, Forensic Science and the Criminal Justice System, 2019: https://publications.parliament.uk/pa/ld201719/ldselect/ldsctech/333/33307.htm

accredited force or service provider. All accreditations to ISO-17025 for forensic science include adherence to ILAC G-19.[53]

83. Working to a recognised international quality standard, demonstrates that systems of working and evidence gathering procedures have been externally assessed against stringent standards and have been deemed competent, robust, consistent and fit for purpose in carrying out and reporting on investigative and testing results. It also facilitates the provision of expert witnesses to the courts who can speak to the underpinning scientific principles and techniques involved in the recovery and analysis of digital evidence. Without validation of its scientific basis, the output from digital forensics will continue to suffer from legitimate questions of validity and reliability.

84. The FSR also has a published Code of Practice and Conduct which providers of forensic scientific evidence are required to follow.[54] Within this there are several milestones which are stipulated for digital forensic laboratories. The standard takes a phased approach to the introduction of accreditation commencing with forensic data acquisition / imaging and extraction of data from hard disk drives, mobile devices and removable media including remote storage.

85. The rationale for making accreditation mandatory followed on from concerns around the validity and reliability of digital evidence being presented to the courts and whether all relevant materials were being disclosed to the defence. One such concern common to Scotland is the issue of evidential screening of digital devices by investigating officers due to the inevitable possibility of unintended confirmation bias.[55] In other words, if investigating officers are 'examining' productions, they will inevitably be looking for data that supports a potential charge. Also, any 'evidential screening' or data extraction will only be as good as the individual officers' ICT skills, particularly if non-accredited systems and processes are in use.

86. Despite training and guidance on the importance of exculpatory evidence, this problem of confirmation bias was highlighted in England and Wales in the high-profile case of student Liam Allan who was cleared of a charge involving six counts of rape in December 2017.[56] In this case it was established by the court that the investigating officer had not examined the digital data on the defendant's phone properly after a defence lawyer found evidence of the phone containing 40,000 text messages which the investigating officer had completely overlooked. One such message established that there had been consensual sex

[53] ILAC G-19, Guidelines for Forensic Science Laboratories, was published in 2002, with the purpose of: "... provide guidance for laboratories involved in forensic analysis and examination by providing application of ISO/IEC 17025." : http://gac.gov.ge/files/ILAC_G19_08_2014.pdf

[54] Forensic Science Regulator, Forensic Science Providers: codes of practice and conduct, 2019: https://www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct

[55] Confirmation bias: A ubiquitous phenomenon in many guises: Nickerson R. S. Review of general psychology 2 (2), 175-220, Sage Journals, (1998)

[56] Rape trial collapses over undisclosed sex messages blamed on police funding cuts, The Independent, 15 December 2017: https://www.independent.co.uk/news/uk/crime/rape-trial-collapse-sex-text-messages-police-funding-cuts-liam-allan-disclosure-phone-innocent-a8113011.html

and exonerated the accused. In this case, the Judge warned of the likelihood of further miscarriages of justice if digital evidence was not properly managed.

87. In a similar case in 2018, another rape trial collapsed after it was established that the police had failed to disclose digital forensic evidence to the defence that would have exonerated the accused.[57] These are just two examples of many from England and Wales which highlight the potential for serious miscarriages of justice if digital forensics techniques and quality management systems are not established and independently accredited. This point was further emphasised in a joint report issued in July 2017 by HM Prosecution Service Inspectorate and HM Inspector of Constabulary (now HMICFRS) which said that even unused items of evidence must be reviewed by the police '…to see whether it is capable of undermining the prosecution case or assisting the defence case', adding: '…If either factor applies it must be disclosed to the defence'.[58]

88. These examples relate to investigations which pre-date accreditation of digital forensics in England and Wales but illustrate why accreditation is necessary to ensure that there are consistent standards applied within the field, and that the Courts may place reliance on the validity and scientific basis for evidence used within the criminal justice system. Overall accreditation is designed to ensure that scientific method translates to increased levels of public confidence and trust in the evidence used within criminal justice.

89. As previously discussed, digital forensics are not yet accredited in Scotland despite recommendation from HMICS in 2017 that they should be. In Scotland, there is a Code of Practice on Disclosure of Evidence in Criminal Proceedings under the Criminal Justice and Licensing (Scotland) Act 2010, Section 164. The Code contains the six core principles of revelation and the six core principles of disclosure. This Code ensures more robust disclosure arrangements in Scotland in relation to all relevant materials.[59] However, Police Scotland has no centralised quality control over the nature, extent or output from digital examinations. Instead, digital examination instructions come via an examination request form from the investigating officer and the onus is on the individual investigating officer to ensure that the rules of disclosure are followed.

90. Notwithstanding, it appears to the DFWG that the juxtaposition of Scotland leading the way in its approach to the accreditation of forensic science but lagging in terms of digital is paradoxical in terms of ensuring the structural integrity of the crime-scene to court model for forensic evidence in Scotland. It also creates an unacceptable political risk of Scotland

[57] London rape trial collapses after phone images undermine case, The Guardian, 15 January 2018: https://www.theguardian.com/law/2018/jan/15/london-rape-trial-collapses-after-phone-images-undermine-case

[58] Making it fair – a joint inspection of the disclosure of unused material in volume Crown Court Cases, July 2017: https://www.justiceinspectorates.gov.uk/hmicfrs/publications/making-it-fair-disclosure-of-unused-material-in-crown-court-cases/

[59] Criminal Justice & Licensing (Scotland) Act 2010 (Section 164): Code of Practice – Disclosure of Evidence in Criminal Proceedings, 2011: https://www.copfs.gov.uk/images/Documents/Prosecution_Policy_Guidance/Guidelines_and_Policy/Code%20of%20Practice%20-%20Disclosure%20of%20Evidence%20in%20Criminal%20Proceedings.pdf

being viewed as operating to a lower standard than has been required by the FSR for England and Wales and raises potential questions around disclosure protocols for cross-border digital evidence sharing.

91. The DFWG therefore concludes that Police Scotland needs to commence a journey of transition with a view to achieving accreditation of its digital forensic laboratory work by December 2022. These aspects and the suggested incremental route to accreditation will be discussed in more detail in the following paragraphs of this report. Although the UKAS website indicates that it is possible for organisations to achieve UKAS accreditation in 6 to 8 months, this longer timescale is advanced in recognition of the scale of Police Scotland, the experience of forces in England and Wales of the accreditation journey, the need for an incremental approach in Scotland, and having regard to potential restructuring towards a new target operating model under the Cybercrime and Technical Surveillance Programme (CTSP).

92. Again, it is emphasised that whilst no system of accreditation can mitigate entirely against individual mistakes, properly accredited and independently assured quality management systems do provide high levels of confidence that no systematic or structural deficits exist. Consequently, the DFWG endorses the need for the accreditation of digital forensic laboratory work in line with the general approach advocated by the Home Office Forensic Strategy, by the FSR for England and Wales, and by previous HMICS recommendation in Scotland connected with ensuring the integrity and value of the crime-scene to court model for forensic evidence in Scotland.

93. In addition, there is also a need for Police Scotland to develop a broader quality framework around non-forensic aspects of digital investigations such as cyber-kiosks or triage technologies. Such a quality framework should ensure the validity and reliability of technologies in use and should also ensure that processes and procedures are ethical, ensuring that there is no bias and that the rules of disclosure in Scotland are complied with. The DFWG acknowledges the significant experience that exists within SPA Forensic Service of such matters and envisages a joint piece of work to develop a quality management framework that is complimentary to the formal accreditation of laboratory work.

Recommendation 3
Police Scotland should commence a journey of transition with a view to achieving accreditation for its digital forensic laboratory work by December 2022. It should also conduct a broader piece of work with SPA Forensic Service to develop a broader quality framework for the non-forensic aspects of digital investigations including triage technologies within the same timescale.

Accreditation - Selecting the most appropriate quality standard

94. The International Organisation for Standardisation (ISO) is the largest publisher of quality standards in the world. These standards are critical for regulating business practices and quality standards. When businesses around the world conform to the same standards

then management techniques, business processes, production controls, quality, products and services all become standardised. ISO has published 23,037 standards and has members in 162 countries, and 788 technical bodies for standard development.[60]

95. The question of which, or indeed whether, any ISO standard is the most appropriate for digital forensics is highly contested by regulators, academics and practitioners alike. In 2019, the House of Lords Science and Technology Select Committee produced a paper entitled; '*Forensic Science and the Criminal Justice System: a blueprint for change'*.[61] Paragraph 81 of the House of Lords report notes the divergence of opinion on the appropriateness of the current accreditation regime for digital forensics in England and Wales. The standard set by the FSR for all forensic science, including digital forensics, is ISO/IEC 17025 which includes adherence to ILAC G-19, which is a quality standard for international laboratory cooperation. The FSR also requires accreditation to adhere to the Codes of Practice and Conduct.

96. Those who argue against ISO 17025 mainly predicate their arguments around ISO 17025 being a standard developed primarily to assess the competence of testing and calibration laboratories, albeit the term 'laboratory' can equally mean an office or workspace. One such argument is that ISO 17025 is being rigidly applied when another standard ISO/IEC 27037 *'Guidelines for identification, collection, acquisition and preservation of digital evidence'* would be the most natural fit. However, this alternative ISO standard appears to the DFWG to be more suitable for digital data security techniques rather than for ensuring the quality and integrity of forensic evidence. The various arguments and debates over which standard is the most appropriate for digital forensics are summarised in the House of Lords paper.

97. The one area on which most commentators agree is that there should be an accreditation standard for digital forensics, and the House of Lords report also notes clear benefits in ensuring that forensic science providers are accredited. As previously discussed, the standard set by the FSR for digital forensics, is ISO/IEC 17025 which includes adherence to ILAC G-19.[62] The FSR also requires those who have accreditation to adhere to the Codes of Practice and Conduct. ISO/IEC 17025 is also the standard for digital forensics advocated by Interpol for policing globally in its *'Global Guidelines for Digital Forensics Laboratories'* document 2019.[63] The Interpol Guidelines extend to 80 pages and provide detailed guidance to police organisations and a universal framework for establishing and managing a digital forensics laboratory/office that is applicable anywhere in the world.

98. Having reviewed the available evidence, the DFWG concludes that accreditation to ISO 17025, (which includes adherence to ILAC G-19) and voluntary adherence to the FSR Codes of Practice, is the quality accreditation framework that should be pursued by Police

[60] ISO, 2019.
[61] Forensic Science and the criminal justice system: A blueprint for change, House of Lords, May 2019: https://publications.parliament.uk/pa/ld201719/ldselect/ldsctech/333/333.pdf
[62] International Laboratory Accreditation Cooperation, ILAC G-19, 2014: ilac.org: http://gac.gov.ge/files/ILAC_G19_08_2014.pdf
[63] Interpol Global Guidelines for Digital Forensic Laboratories, Singapore, 2019

Scotland for its digital forensic laboratory work. This will ensure that the quality standard adopted by Police Scotland for digital forensics align with those for forensic science in Scotland, thus delivering a consistency of approach over all forensic disciplines to further strengthen the quality and integrity of the crime-scene to court model in Scotland. This approach will also ensure alignment with the approach to accreditation by policing in England and Wales, and to the standard advocated for policing globally by Interpol. We acknowledge that the journey towards accreditation involves significant changes in management and culture and would expect SPA Forensic Service to actively assist Police Scotland in the process of accreditation, using the skills and experience they have developed.

Recommendation 4
Police Scotland should adopt the ISO 17025 quality standard for accreditation of its digital forensic laboratory work in Scotland by December 2022.

Recommendation 5
On attaining the ISO 17025 quality standard accreditation for its digital forensic laboratory work, Police Scotland should voluntarily adhere to the Forensic Science Regulators Codes of Practice and Conduct as mandated for Forensic providers, including policing in England and Wales.

Accreditation – Inclusions, exclusions and incremental changes

99. Before turning to consider the necessary steps towards accreditation of digital forensics it is necessary to briefly discuss four main questions which have arisen as part the DFWG external and internal stakeholder engagement and consultation. Those four questions are:

- What aspects of digital data investigation by the police should be included and excluded from the scope of digital forensics accreditation?
- What is the learning from the accreditation journey in England and Wales?
- Does the process of accreditation negatively impact on the existing capacity and capability of digital forensics disciplines without additional project resources?
- Are there advantages in an incremental approach to accreditation?

100. In considering these four questions arising from consultation it is useful firstly to reflect on the purpose of accreditation for digital forensics. For Scotland, that purpose would be to deliver an independently validated consistency of approach over all forensic disciplines, to further strengthen the quality and integrity of the crime-scene to court model. It follows from this strategic imperative that accreditation should apply to all digital evidence that is extracted from digital storage media, rendered into a useable form, and then processed and interpreted for the purpose of obtaining intelligence or evidence in line with the FSR definition discussed previously.

101. It also follows logically that different rules would apply to digital investigations which are non-forensic, and do not involve extraction of digital evidence from digital storage media. One such example is in relation to open source intelligence, also known as Internet Intelligence and Investigations. This term covers three levels of activity:

- Core internet use
- Overt internet intelligence and investigations
- Authorised covert intelligence and investigations

102. As these are investigative activities and not 'forensic' activities they do not require to be accredited and they are not considered further by the FSR.[64] This means that Internet Intelligence Investigations, including investigations of criminal use of the Dark Net and Deep Web where custom criminal software and hidden networks are superimposed on the architecture of the Internet would be exempt from any scheme of accreditation.

103. In relation to cyber-kiosks or digital triage devices, Police Scotland has published information which explains that it uses these desktop computers containing specialist software to enable trained officers to view information on a mobile phone or tablet, which may be relevant to a police investigation or incident. If evidence is identified on a device, it will be submitted to a Digital Forensic Hub for further examination and preparation for court. If in the opinion of the operating officer it does not, Police Scotland may be able to return the device to its owner.

104. Since Police Scotland restricts the use of cyber-kiosks to viewing material on a mobile phone or tablet then it may be legitimately argued that their use by Police Scotland is solely evidential screening and non-forensic in nature. However, this returns us to debates earlier in this DFWG report about the issues of confirmation bias and the need to afford equal weight to exculpatory evidence to fulfil disclosure obligations. Therefore, there are clearly limitations to the value of such technologies, particularly when deployed without manual verification, as is inevitably the case when used by front-line police officers.

105. In a broader UK context, there has been continued focus from the NPCC digital forensics portfolio to explore options to validate kiosk technology. In the 2019 Annual Report, the FSR notes that understanding the limitations of kiosk technologies depending on the make and model of the mobile phone or tablet being examined, will greatly assist the police in ensuring whether reasonable lines of enquiry have been pursued. Consequently, it will assist the police in fulfilling their disclosure obligations. The FSR has also said that '…only one deployment per force needs be on the schedule of accreditation providing the force can control further deployments and training of its users'.[65]

106. At this time, and solely within the context of their evidential screening use by Police Scotland, it is the opinion of the DFWG that cyber-kiosks are a pre sterile corridor and non-forensic investigative screening activity and that they should not require to be the subject of

[64] Forensic Science Regulator, Annual Report 2018, pages 21-22: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786137/FSRAnnual_Report_2018_v1.0.pdf

[65] *Ibid,* page 26, paragraph 2.2.

formal ISO accreditation mechanisms. However, this should be kept under review by Police Scotland pending wider UK developments under the NPCC digital forensics portfolio. Police Scotland should however have appropriate quality control mechanisms in place around all non-forensic digital activity. Such systems, processes and procedures should include validated mechanisms to identify and record mistakes or bias, to confirm the continued validity and reliability of standard operating procedures and protocols, and to ensure that best practice and the rules of disclosure are being followed.

107. Having discussed potential exclusions from accreditation in terms of pre sterile corridor and non-forensic digital activity, it therefore follows that the opinion of the DFWG is that all post sterile corridor digital forensics should be accredited by Police Scotland. In time, this should include the full range of activities conducted within the 5 Digital Forensic Hubs where that forensic activity feeds into the criminal justice system in Scotland. For the avoidance of doubt, this means that after an item has been labelled as a production and submitted to a Digital Forensic Hub via a Digital Forensic Gateway, then the subsequent digital forensic examination and analysis should fall within the scope of accreditation.

108. However, drawing on the learning from England and Wales it is clear to the DFWG that an incremental and phased approach will be required. The experience in England and Wales, and slower than anticipated pace of progress has often resulted from competing priorities with other forensic demands, and often because the implementation of a quality management system has not been viewed as a priority and has not been resourced appropriately.

109. For these reasons, many police forces in England and Wales currently hold accreditation solely for a specified sub-discipline, focussing first on computers and associated media, or alternatively on mobile phones and tablets. A full list of which force or providers of forensic services to policing holds which accreditation in the UK can be seen on the UKAS website.

110. In recommendations 3, 4 and 5 of this DFWG report we recommend that Police Scotland should seek to achieve ISO 17025 accreditation in its digital forensic laboratory work by December 2022. We also suggest this timeframe in recognition of the scale of Police Scotland, the experience of forces in England and Wales of the accreditation journey, the need for an incremental approach in Scotland, and having regard to potential restructuring towards a new target operating model under the Cybercrime and Technical Surveillance Programme (CTSP).

111. As it would appear to the DFWG from available Police Scotland data that mobile phones account for significantly the largest percentage of devices submitted to the Digital Forensic Hubs (currently 86% to 90%) for digital forensic examination, it would appear logical for Police Scotland to commence its accreditation journey with this sub-discipline with a view to achieving UKAS accreditation in phones as a minimum by December 2022. Ultimately however, these are operational decisions for Police Scotland that will be influenced by a range of other factors including finance, progress with CTSP, and the availability of a dedicated resource or resources to project manage the selected

accreditation journey. A regulation and standards schematic for digital forensics showing the various ISO standards is attached as **Appendix 4** to this report.

112. Whilst beyond the scope of the terms of reference for the DFWG, there is clearly a need for significant investment in the digital space if Scotland is to keep pace with the trajectory of digital growth including the volumes and complexity of data, and the diversity of devices and cloud-based storage media. The digital age is fundamentally changing not only our social structure but also prevailing modes of criminality and demands new ways of thinking. In the digital age conventional boundaries no longer matter, the opportunities and threats are the same whether you are in Leith or Lerwick. Policing in the digital age is not just about policing, it is also a problem for government, for those with an interest in privacy, ethics and human rights, for academia, for the public and private sectors, and of course for civil society.

Accreditation - The steps to UKAS Accreditation, timescales and costs

113. The route to accreditation is fully described on the UKAS website. This includes a step-by-step guide through the key steps of the accreditation process. The site also gives access to the supporting information needed at each stage of the application, as well as access to information about potential costs and timescales. It also includes information on how to maintain accreditation status, extend the scope, and how to get the most value from being an accredited organisation.[66]

114. UKAS emphasise that the route to accreditation is not as daunting as it might initially appear, and applicant bodies are assisted through the process by a UKAS appointed assessment manager. In Scotland, Police Scotland would also have access to significant experience within the SPA Forensic Service of the route to accreditation. The route to UKAS accreditation is summarised by the following 10 steps:

Step No:	Description
1	The applicant organisation must be based in the UK.
2	Determine the most appropriate ISO standard required (ISO 17025) and purchase and download the standard from the British Standards Institute (BSI) website.
3	Familiarise with clauses and requirements of the international standard and supporting UKAS guidance materials, then self-conduct a gap analysis against existing processes and procedures. Close any obvious gaps.
4	Gather the necessary documentation and evidence to support an application.
5	Submit application to UKAS together with supporting documents and information.
6	UKAS will appoint an Assessment Manager to support and guide the application.
7	Opportunity for optional pre-assessment to identify residual gaps.
8	Formal assessment commencing with opening meeting to finalise assessment arrangements. UKAS then reviews procedures and records, meets the team and assesses how well the organisation is working towards meeting the relevant international standard.
9	UKAS provides detailed assessment report & improvement plan if necessary.

[66] UKAS, the route to accreditation, 2020: https://www.ukas.com/the-route-to-accreditation/

10	Residual gaps are closed within 12 weeks. UKAS grants accreditation, issues certificate and organisation will be added to list of accredited bodies on UKAS website. Organisation can use UKAS symbols and those trading internationally can use ILAC to signal global acceptance.

Figure No 6: UKAS 10 Steps to Accreditation

115. As discussed earlier in this report, it is possible for organisations to achieve UKAS accreditation in 6 to 8 months, however the DFWG is suggesting a longer timescale in recognition of the scale of Police Scotland, the experience of forces in England and Wales of the accreditation journey, the need for an incremental approach in Scotland, and having regard to potential restructuring towards a new target operating model under the Cybercrime and Technical Surveillance Programme (CTSP).

116. In terms of the costs associated with accreditation of digital forensics by Police Scotland it is not possible to give an exact amount, but indicative calculations can be made from case study data on the UKAS website. The relevant financial examples are based on a 2018/19 price list and are exclusive of VAT. The various UKAS examples are estimates provided for guidance purposes only. UKAS provides a bespoke quote for each customer based on their specific application and circumstances. In addition, there are initial costs associated with the accreditation, then recurring costs to maintain accreditation via surveillance assessments in each of years 1 to 3, and a reassessment in year 4.

117. Based on case-study data, the DFWG believes that it would be reasonable to anticipate the following costs for the accreditation of digital forensics by Police Scotland:

Item	Approximate cost (£)	Fiscal Year
Purchase of ISO standard from BSI website	130	2020/2021
Application fee	2,000	2021/2022
Pre- Assessment (optional)	12,000 to 18,000	2021/2022
Initial Assessment	24,000 to 36,000	2022/2023
Surveillance Assessment 1	12,000 to 18,000	2023/2024
Surveillance Assessment 2	13,000 to 20,000	2024/2025
Surveillance Assessment 3	13,500 to 20,250	2025/2026
Reassessment (Year 4)	18,000 to 27,000	2026/2027

Figure No 7: Potential Costs associated with UKAS accreditation for Digital Forensics

118. As indicated, UKAS would provide Police Scotland with a bespoke quote at the time of application and the indicative costs above may vary significantly if the target operating model for CTSP increases the existing number of Digital Hubs. However, based on the above calculations it would seem reasonable to project average annual costs associated with the ongoing accreditation of digital forensics in a range from £20K to £30K per annum. This is comparable with the current annual costs associated with the SPA Forensic Services accreditation which is in the region of £120K per annum. It should be noted that the above costs are for the accreditation process only. They do not include additional capital or revenue costs that may be identified from a gap analysis of existing facilities, technology, procedures or processes conducted against the relevant international standard.

Ethical and human-rights considerations

119. The ethical and human rights considerations which arise in relation to digital forensics and policing are almost identical to those which arise in relation to the acquisition, use, retention and disposal of biometric data. As previously discussed, digital forensic techniques can give access to highly sensitive personal data, including enabling the police to overcome biometric access controls on certain devices, and gaining direct access to biometric data within devices such as photographs.

120. With this in mind, we were fortunate enough to be able to draw on the knowledge and expertise of several individual DFWG members and organisations who had also been part of the Independent Advisory Group (IAG) on Biometric Data in Scotland which had been chaired previously by prominent solicitor advocate John Scott Q.C.

121. The report of the IAG on Biometric Data was published in March 2018 and made nine recommendations to Scottish Government. This included bringing forward legislation to introduce an independent Biometrics Commissioner for Scotland, a statutory requirement for a Code of Practice, and several ethical and human rights considerations including the presumption of deletion of data where persons were not convicted. Recommendations also included special considerations for children and vulnerable groups, and improved legislation. The final recommendation of the IAG was that an ethics advisory group should be established by Scottish Ministers as part of new independent oversight arrangements. The intention behind the Ethics Advisory Group recommendation was to provide independent ethics and human rights advice in a way broadly like that which is provided to the Home Office in England and Wales by the Biometrics and Forensic Ethics Group (BFEG). This group should work with the Commissioner and others to promote ethical considerations in the acquisition, retention, use and disposal of biometric technologies and biometric data.[67]

122. Following the report of the IAG, Scottish Government brought forwards a Bill to introduce a Scottish Biometrics Commissioner and a Code of Practice.[68] The Scottish Government Bill was introduced by Cabinet Secretary for Justice, Humza Yousaf MSP, on 30 May 2019. The Bill completed Stage two on 4 February 2020 and completed Stage 3 passing into legislation on 10 March 2020 with every MSP present voting in favour of the Bill. The next stage will be for the Scottish Parliament Corporate Body to run a selection process to appoint the new Commissioner. One of the first tasks of the new Scottish Biometrics Commissioner will be to develop a Code of Practice that embodies human rights and ethical considerations in consultation with Police Scotland, the SPA and others. The Scottish Biometrics Commissioner will then monitor compliance with the Code and report on progress to the Scottish Parliament.

[67] Independent Advisory Group on the use of Biometric Data in Scotland, March 2018: https://www.gov.scot/binaries/content/documents/govscot/publications/independent-report/2018/03/report-independent-advisory-group-use-biometric-data-scotland/documents/00533063-pdf/00533063-pdf/govscot%3Adocument/00533063.pdf

[68] Scottish Biometrics Commissioner Bill, Scottish Parliament 2019: https://www.parliament.scot/parliamentarybusiness/Bills/111859.aspx

123. During the passage of the Bill, the Scottish Parliament subsequently agreed that there will be a statutory Advisory Group to support the Commissioner. This Group will be appointed by the Commissioner and will provide advice on any matters relating to the functions of the Commissioner.

> *'Technological advances in biometrics have brought huge benefits to police and other justice agencies in detecting, preventing and prosecuting crime. However, their use also raises several ethical and human rights considerations. The Scottish Government wants to ensure that the approach to biometric data in policing and criminal justice system is lawful, effective and ethical'*
>
> *(Cabinet Secretary for Justice, 30 May:2019)*

124. As many digital forensics processes will contain biometric data, the DFWG welcomes the arrangements to be put in place following the appointment of a Scottish Biometrics Commissioner as adherence to that Code of Practice by Police Scotland, and other specified agencies, will also deliver additional ethical and human rights safeguards around digital forensics.

125. In terms of the human rights and ethical principles pertaining to both biometric and forensic data, BFEG in England and Wales, and subsequently the IAG on Biometric Data in Scotland have highlighted a number of principles that should enhance trust in the use of biometric and forensic services. In April 2018, BFEG published a series of 'Principles' that considered moral, legal and social policy considerations.[69] The guidelines provided by BFEG, and subsequently the Scottish IAG address:

- Governing principles for forensic and biometric procedures
- Human rights and ethical considerations when implementing the governing principles
- Considerations specific to the collection and processing of data

126. The DWG is of the opinion that the seminal work of the IAG on Biometric Data in Scotland, and subsequent progress by Scottish Government, has already put in motion a series of events that will inevitably lead to stronger and more independent oversight, governance and assurance around how sensitive biometric and forensic data is used by policing in Scotland. These measures will undoubtedly strengthen and enhance human rights and ethical considerations.

127. The DFWG also concludes that work by Police Scotland through the CTSP Programme offers the potential to improve both the visibility and quality of internal governance arrangements within Police Scotland, which as a corollary will also reinforce SPA oversight. Cumulatively, these various opportunities for improvement will enable digital forensics to flourish in a way that balances the needs of citizen and state through strong

[69] Biometrics & Forensics Ethics Group (BFEG), Ethical Principles, April 2018: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702184/Biometrics_and_Forensics_Ethics_Group_principles_website_v2.pdf

internal governance, strengthened SPA oversight, supported by accreditation to an international quality standard, and with robust and independent oversight.

Summary of DFWG external consultation and engagement

128. There are several methodological difficulties associated with social research and policing as it often engages with niche audiences with highly polarised opinions. Recognising those constraints, the DFWG engaged widely with a range of interest groups, practitioners, regulators, policy makers, academia, human rights advocates and many others whose valuable insights and experience have helped to shape the content of this report. As highlighted in the Executive Summary of this report, external consultation and engagement formed part of the design of this review and we consulted widely and extensively from the outset.

129. In addition to various bi-lateral communications and discussions, the DFWG organised and hosted 2 distinct consultation and engagement events to ground our broader research findings in Scotland against the experience and opinions of practitioners and others with relevant subject expertise in relevant areas. **Appendix 2** summarises the dates of these events.

130. The first event was a symposium of practitioners with additional representation from Scottish Government, the Scottish Information Commissioner, Leverhulme Institute, the Children and Young People's Commissioner, HMICS and members of the SPA Board. The event took the form of semi-structured focus groups and the views of practitioners were sought on a range of issues under the general theme of operational readiness.

131. The second event was a symposium of subject experts with relevant expertise in the law, privacy, ethics, academia and human rights. This event also took the form of semi-structured focus groups. Research questions for discussion included:

- How should we balance the needs of the justice system with the rights of individuals when designing a digital forensics service? And.
- What are the key ethical and human rights issues around digital forensics and how should they be mitigated against as digital forensics develops?

132. Perhaps surprisingly, there was a good level of consensus over both symposiums as to the essential components of a sound system of necessary ethical and human rights safeguards. These aggregated areas of consensus are summarised as follows:

- Systems for assessing digital content should be proportionate and necessary having regard to the specific matter under investigation and must be justifiable in law
- Systems and procedures around digital forensics must be values and ethics based
- There should be clear search parameters around digital forensics to safeguard against unnecessary collateral intrusion

- Accreditation and quality assurance mechanisms are viewed as essential in order to ensure that the underlying scientific approach is credible and that the results of searches are based on reliable and valid techniques
- There is a need to ensure that processes do not discriminate. Such processes need to be quality assured to preclude the possibility of confirmation bias, and to ensure that the rules of disclosure in Scotland are complied with
- Accreditation to ISO standard was viewed as important, as was the need for Scotland to follow broader Scottish, UK and international models of forensic accreditation. Complimentary quality management systems were viewed as important for non-forensic areas of digital investigations
- Without accreditation, Scotland lags in digital forensics. This has potential implications for the perceived validity and reliability of digital evidence, rules of disclosure and the weight that the courts should attach to so-called expert witnesses. Accreditation was essential to safeguard against potential allegations of digital in Scotland being 'Junk-Science'.

133. In conclusion, the strategic message from both consultation events, and from our fuller consultation and engagement with a range of stakeholders was that further work was required to better balance the needs of law enforcement with the civil rights of private citizens through externally validated, regulated, and quality assured systems, which in turn facilitate enhanced public confidence and trust in digital policing activity.

Appendix 1: Membership of DFWG

The undernoted individuals formed the core membership of the SPA Digital Forensics Working Group. In addition to the core membership, other representatives from the various participating agencies assisted as and when required:

Robert Hayes, SPA Board Member	Chair of DFWG
Jane Ryder, SPA Board Member	DFWG Lead on Engagement
Tom Nelson	SPA Director of Forensic Services
ACC Angela McLaren	Police Scotland
ACC Roddy Irvine	HMICS/Police Scotland
Andrew Richardson	COPFS
Detective Supt Nicola Burnett	Police Scotland
Martin Mackay	HMICS
Detective Ch Supt Gary Cunningham	Police Scotland
Kevin O'Hare	Scottish Police Authority
Kevin Murray	HMICS
Detective Supt Raymond Higgins	Police Scotland
David Scott	Scottish Government (Secretariat)
Dr Brian Plastow	SPA Project Support

Appendix 2: List of DFWG meetings and consultation/engagement events

The following schedule lists the meeting dates of the DFWG and the dates of formal consultation and engagement with key stakeholders:

Meetings of DFWG	
13 September 2019	Scottish Crime Campus
6 November 2019	Edinburgh
4 February 2020	Edinburgh
20 March 2020	Edinburgh
Stakeholder Consultation and Engagement Symposiums	
22 January 2020	**Operational Readiness** This consultation and engagement symposium were aimed at operational practitioners and 20 delegates were in attendance. This included representation from: • Police Scotland • SPA Board • SPA Forensic Services • Scottish Government • Scottish Information Commissioner • Leverhulme Institute, University of Dundee • Children & Young People's Commissioner • HMICS
24 February 2020	**Governance, Human-Rights, Ethics, Public Trust and Confidence** This consultation and engagement symposium were aimed at a broad spectrum of external and internal stakeholders with an interest in contemporary debates around digital forensics and 25 delegates were in attendance. This included representation from: • Scottish Human Rights Commission • Leverhulme Institute University of Dundee • Abertay University • Napier University

	• Children & Young People's Commissioner Scotland • Scottish Government • Scottish Police Authority • COPFS • HMICS

Appendix 3: Regulation & Standards Schematic

Regulation & Standards in Digital Forensics

	Cyber-Essentials	Cyber-Essentials Plus	ISO 27001	ISO 17020	ISO 17025	Forensic Regulator Code of Practice
	ICT infrastructure security		Information security	Inspection and testing standard		Good practice standard
Requirement	• Cyber Essentials is ideal for smaller businesses looking to understand their current cyber defences. • Government program in the U.K. • Current version: Cyber Essentials 2015 • Defines a set of controls that cover the basics of cyber security related to common Internet-originated attacks against an organization's IT systems, and a mechanism to demonstrate that these precautions have been taken. • The **five technical security controls** are: - Firewalls - Secure configuration - User access control - Malware protection - Patch management • Applicable to any type and size of organization. • Implementation and certification are mandatory for UK government suppliers contracted for handling sensitive and personal information. For other purposes, they are optional. • CA certification award based on a **self-assessment** questionnaire regarding compliance with the Cyber Essentials control themes, approved by a senior executive (e.g., CEO), which is verified by an independent NCSC certified external **certification** body. This option offers a **basic** level of assurance and can be achieved at a low cost.	• Cyber Security Plus certificate has the **same requirements** as the basic certificate. • The 'Plus' certificate requires an **independent** assessment of security controls. This is to verify that these five checks are in place. • As a result of its external verification measures, the Cyber Essentials Plus certificate is often regarded as the more reliable certification. • Defines the **same set of controls** that cover the basics of cyber security related to common Internet-originated attacks against an organization's IT systems, and a mechanism to demonstrate that these precautions have been taken • Applicable to any type and size of organisation. • Certification awarded based on external testing of the **organisation's cyber security approach**, performed by an independent NCSC certified external **certification** body. • This option costs more (dependent on size and complexity of organisation) than the Cyber Essentials certification, but offers a higher level of assurance.	• ISO 27001'Information technology. Security techniques. Information security management systems. Requirements' is an international information security standard, recognised worldwide in different jurisdictions and industries. • The very nature of any international standard is that it must be able to address all circumstances in which the standard might be used. This means it has to be very extensive and comprehensive, and this in turn leads to complexity and expense. • Includes over **100 controls**, the standard is frequently implemented by corporations or businesses dealing with **critical infrastructure or the public sector**. • ISO 27001 covers areas that include security policies, access control, operations security, human resources, cryptography and compliance. • It is a **comprehensive assessment** of a whole organisation's ability to look after information securely in **all contexts**. • It is therefore likely that the type of organisation that would choose to implement this standard would be, for example, large in business function or personnel, and/or would have major quantities of sensitive information they want to protect, and/or need to prove they are looking after other people's information appropriately. • One aspect of ISO 27001 is that it does not provide detail on what to do to fulfil requirements or implement controls; it only tells you what you need to achieve. • Bodies providing Certification services for ISO 27001 are assessed by the **United Kingdom Accreditation Service (UKAS).**	• ISO/IEC 17020:2012 'Conformity assessment – Requirements for the operation of various types of bodies performing inspection'. • Accreditation provides formal recognition that an inspection service is capable of meeting the **standards of quality, performance, technical expertise, competence** and **professional judgement**. • Companies accredited to this standard can: - perform inspections, - compile sampling plans, - take samples, - send these samples to an accredited organisation for analysis. • UKAS accreditation minimises the risk of inaccurate inspection results, providing confidence to customers, stakeholders and the public, through external evaluation by an **independent, third party** body. • This Standard, through **clauses 6.2.13, 7.1.7 and 7.1.8,** provides structure to the **Capture and Preservation** phase of the Digital Forensic Process through definition of the digital forensic strategy. The purpose of this is to prevent loss or change to digital evidence taken from the scene. The use of adequately controlled methods to prevent unwanted changes is key to prevent the evidence becoming unusable later. • **Examination of a Digital Scene** using fit for purpose, validated equipment, utilised by trained and competent staff, using their professional judgement and experience will identify and prioritise the recovery of forensic digital evidence. This will include the range of relevant examinations available and assessing those most likely to achieve the most positive forensic outcomes within the specific situation. • **Accreditation** to the **Standard** is performed by **UKAS** by on site assessment over a number of days by **technically competent** assessors.	• ISO/IEC 17025:2017 'General requirements for the competence of testing and calibration laboratories' • Laboratory accreditation is the process of assessing and endorsing the **quality management and technical competence** of **testing, measurement** and **calibration laboratories** in all fields of **science** and **technology**. These include biology, chemistry, metrology and calibration. • Companies accredited to this standard can: - take samples, if included in their accreditation, - analyse samples, - issue factual reports on their findings. - provide opinions, interpretations, assessments and / or certifications as to the meaning of these results. • UKAS accreditation **minimises** the risk of **inaccurate** testing **results**, providing confidence to stakeholders and the public, through external evaluation by an **independent, third party** body. • Through **clause 7.11,** the Standard provides structure to the **Testing, Evaluation and Reporting** phase of the Digital Forensic Process through handling, chain of custody and effective case management, as well as use of maintained and calibrated equipment and methods. Use of QC measures to produce a reliable, fully traceable, result provides assurance to the Criminal Justice System. • Clause 7.8.7, allows the laboratory to draw conclusions that are based on more than just the result of the test at hand, for example conclusions drawn from observations at a scene of crime. The consideration of one or more alternative hypotheses allows an organisation to demonstrate its impartiality. • **Accreditation** to the **Standard** is performed by **UKAS** by on site assessment over a number of days by **technically competent** assessors.	• The Code of Practice aligns with ISO 17025:2005 (as interpreted by ILAC G19:08/2014 Modules in a Forensic Science Process) and specifies the **requirements for a management system** for forensic units. • The Forensic Science Regulator expects activities, **wherever performed**, to be conducted to the standards set out in the Codes, irrespective of whether the provider is public, police or commercial. • Digital forensics is the process by which information is extracted from data storage media, rendered into a useable form, processed and interpreted for the purpose of obtaining intelligence for use in investigations, or evidence for use in criminal proceedings. This **definition** is **intentionally wide** and any exclusions will be explicit. • Clause 21; Control of data applies, together with: - FSR-C-107 - Appendix: Digital Forensic Services, - FSR-G-218 – Method Validation in Digital Forensics, - FSR-R-648 - Advice from the National Cyber Security Centre on potential new text for the Control of Data section of the Regulator's Codes of Practice and Conduct (consultation). • UKAS will assess forensic units providing forensic science services against **ISO 17025, relevant UKAS publications, ILAC G19** and the **supplementary requirements** of the Code of Practice.
	Both ISO 27001 and Cyber Essentials aim for information protection, but while ISO 27001 considers information regardless of where it is found (e.g., paper, information systems, digital media, etc.), Cyber Essentials focuses on protection of data and programs on networks, computers, servers, and other elements of an IT infrastructure.			Third party assessment by UKAS accreditation offers confidence that forensic activities are carried out impartially and competently. Compliance infers the highest standards of personal conduct and organisational compliance with quality standards.		

Appendix 4: Glossary of Terms

BFEG	Biometrics & Forensics Ethics Group
CCP	Cybercrime Capability Programme
CCTV	Closed Circuit Television
COPFS	Crown Office and Procurator Fiscal Service
CSAE	Child Sexual Abuse and Exploitation
CSE	Child Sexual Exploitation
CSEM	Child Sexual Exploitation Material
CTSP	Cybercrime & Technical Surveillance Programme
DESC	Digital Evidence Sharing Capability
DFE	Digital Forensic Examiner
ERF	Examination Request Form
DNA	Deoxyribonucleic Acid
FOI	Freedom of Information
FSC	Forensic Services Committee
FSR	Forensic Science Regulator
GPS	Global Positioning System
HMICFRS	HM Inspectorate of Constabulary Fire & Rescue Service
HMICS	Her Majesty's Inspectorate of Constabulary (Scotland)
IAG	Independent Advisory Group
ICT	Information and Communications Technology
ILAC	International Laboratory Accreditation Cooperation
IDENT1	UK Fingerprint Database
IIU	Internet Investigations Unit
IOCTA	Internet Organised Crime Threat Assessment
ISO	International Organisation for Standardisation
MSP	Member of the Scottish Parliament
NCA	National Crime Agency

NDNAD	National DNA Database
NPCC	National Police Chief's Council
OCCTU	Organised Crime & Counter Terrorism Unit
PIRC	Police Investigations and Review Commissioner
QMS	Quality Management System
SCD	Specialist Crime Division
SCRO	Scottish Criminal Records Office
SFI	Standard Fiscal Instruction
SGEM	Self-Generated Explicit Material
SIO	Senior Investigating Officer
SPA	Scottish Police Authority
TIU	Telecommunications Investigation Unit
TOM	Target Operating Model
TS21C	Technical Surveillance for 21st Century Programme
UKAS	UK Accreditation Service
VAT	Value Added Tax

Appendix 5: Bibliography

ACPO Good Practice Guide for Digital Evidence, Association of Chief Police Officers (2012).

Alternate Data Storage Forensics, A. Schroader & T. Cohen (2007)

An examination of Digital Forensic Models. Reich *et al* (2002)

Audit Scotland, the 2018 Audit of the SPA Section 22 Report: https://www.audit-scotland.gov.uk/report/the-201819-audit-of-the-scottish-police-authority

Biometrics & Forensics Ethics Group (BFEG), Ethical Principles, April 2018: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702184/Biometrics_and_Forensics_Ethics_Group_principles_website_v2.pdf

Confirmation bias: A ubiquitous phenomenon in many guises: Nickerson R. S. Review of general psychology 2 (2), 175-220, Sage Journals, (1998)

Criminal Justice & Licensing (Scotland) Act 2010 (Section 164): Code of Practice – Disclosure of Evidence in Criminal Proceedings, 2011: https://www.copfs.gov.uk/images/Documents/Prosecution_Policy_Guidance/Guidelines_and_Policy/Code%20of%20Practice%20-%20Disclosure%20of%20Evidence%20in%20Criminal%20Proceedings.pdf

Cyber-crime in Scotland: A Review of the Evidence, Scottish Government Crime and Justice Social Research, March 2018: https://www.gov.scot/publications/cyber-crime-scotland-review-evidence/

Digital and Cybercrime, College of Policing, 2020: https://www.college.police.uk/What-we-do/Learning/Professional-Training/digital-and-cyber-crime/Pages/Digital-and-cyber_crime.aspx

Digital Forensics and Crime, Houses of Parliament, Parliamentary Office of Science and Technology, Post number 520, March 2016: https://researchbriefings.files.parliament.uk/documents/POST-PN-0520/POST-PN-0520.pdf

Digital Forensics Literature Review for DFWG, prepared by Dr Brian Plastow, October 2019 (unpublished).

Europol, European Cybercrime Centre – Combating Crime in a digital age (2019)

Fingerprint Service in Scotland leading the way in the UK, December 2016: http://www.spa.police.uk/news/437866/373775/

Forensic Big Data Analytics, Netherlands Forensic Institute, forensicinstitute.nl

Forensic Science and the criminal justice system: A blueprint for change, House of Lords, May 2019: https://publications.parliament.uk/pa/ld201719/ldselect/ldsctech/333/333.pdf

Forensics Review: Review of the provision of forensic science to the criminal justice system in England and Wales, Home Office: July 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/800447/Joint-review-of-forensics-provision-July-2018.pdf

Forensic Science Regulator, Annual Report 2018, pages 21-22: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786137/FSRAnnual_Report_2018_v1.0.pdf

Forensic Science Regulator, Forensic Science Providers: codes of practice and conduct, 2019: https://www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct

Forensic Science Regulator, Newsletter 26, October 2015: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/470526/FSR_Newsletter_26__October_2015.pdf

Forensic Science Strategy: A national approach to forensic science delivery in the criminal justice system, Home Office, 2016: https://www.gov.uk/government/publications/forensic-science-strategy

HMICS Thematic Inspection of the SPA Forensic Service, 27 June 2017: https://www.hmics.scot/publications/thematic-inspection-scottish-police-authority-forensic-services

HM Treasury Green Book, 2018: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/685903/The_Green_Book.pdf

Home Office, Biometrics and Forensics Ethics Group (BFEG) : https://www.gov.uk/government/organisations/biometrics-and-forensics-ethics-group

House of Lords, Forensic Science and the Criminal Justice System, 2019: https://publications.parliament.uk/pa/ld201719/ldselect/ldsctech/333/33307.htm

Independent Advisory Group on the use of Biometric Data in Scotland, March 2018: https://www.gov.scot/binaries/content/documents/govscot/publications/independent-report/2018/03/report-independent-advisory-group-use-biometric-data-scotland/documents/00533063-pdf/00533063-pdf/govscot%3Adocument/00533063.pdf

International Laboratory Accreditation Cooperation, ILAC G-19, 2014: ilac.org: http://gac.gov.ge/files/ILAC_G19_08_2014.pdf

ILAC G-19, Guidelines for Forensic Science Laboratories, was published in 2002, with the purpose of: "... provide guidance for laboratories involved in forensic analysis and

examination by providing application of ISO/IEC 17025." : http://gac.gov.ge/files/ILAC_G19_08_2014.pdf

Improving Digital Evidence Sharing, DESC Programme, Scottish Government, 2019: https://www.gov.scot/news/improving-digital-evidence-sharing/

Information for Prospective Bidders, Metropolitan Police Service – Digital Cyber and Communications Forensics Unit (2015).

Interpol, Global Guidelines for Digital Forensic Laboratories, Interpol (2019)

IOCTA 2019, Europol EC3 Cybercrime Centre: https://www.europol.europa.eu/iocta-report

Justice in Scotland: Vision and Priorities, Scottish Government, July 2017: https://www.gov.scot/publications/justice-scotland-vision-priorities/

London rape trial collapses after phone images undermine case, The Guardian, 15 January 2018: https://www.theguardian.com/law/2018/jan/15/london-rape-trial-collapses-after-phone-images-undermine-case

Making it fair – a joint inspection of the disclosure of unused material in volume Crown Court Cases, July 2017: https://www.justiceinspectorates.gov.uk/hmicfrs/publications/making-it-fair-disclosure-of-unused-material-in-crown-court-cases/

Man who groomed and raped girls in Edinburgh jailed, BBC, March 2019: https://www.bbc.com/news/uk-scotland-edinburgh-east-fife-47415703

Metropolitan Police outsource Digital Forensics in seven year deal worth £8 million: ComputerWeekly.com: https://www.computerweekly.com/news/450422403/Met-Police-signs-8m-digital-forensics-deal

MSP's call for police 'cyber-kiosk' rollout to be paused, Scottish Parliament Justice Sub-Committee on Policing, 08 April 2019: https://www.parliament.scot/newsandmediacentre/111642.aspx

National Crime Agency (NCA), National Strategic Assessment of Serious and Organised Crime, 2019: https://nationalcrimeagency.gov.uk/who-we-are/publications/296-national-strategic-assessment-of-serious-organised-crime-2019/file

Netherlands Forensic Institute: https://www.forensicinstitute.nl/

Police and Fire Reform (Scotland) Act 2012, paragraph 31

Police Scotland Annual Police Plan 2019-2020: Serving a Changing Scotland: https://www.scotland.police.uk/assets/pdf/138327/150739/annual-police-plan-2019-20?view=Standard

Police Scotland cyber kiosks, policies, legal basis and impact assessments, 2020: https://www.scotland.police.uk/about-us/police-scotland/specialistcrime-division/cybercrime-investigations-digital-forensics/cyber-kiosks

Police Scotland, Procurement Strategy 2017-2020: https://www.scotland.police.uk/assets/pdf/138327/327595/procurement-strategy-2017-2020

Police urged to abandon facial recognition scans, The Times, 20 May 2020.

Rape trial collapses over undisclosed sex messages blamed on police funding cuts, The Independent, 15 December 2017: https://www.independent.co.uk/news/uk/crime/rape-trial-collapse-sex-text-messages-police-funding-cuts-liam-allan-disclosure-phone-innocent-a8113011.html

Realising Scotland's full potential in a digital world: A Digital Strategy for Scotland, Scottish Government, 2017: https://www.gov.scot/publications/realising-scotlands-full-potential-digital-world-digital-strategy-scotland/

Response to FOI request by Police Scotland, published 26 January 2020, The Ferret: https://theferret.scot/police-scotland-backlog-digital-forensic-analysis/

Restricted briefing paper to ACC Organised Crime, Counter Terrorism and Intelligence, February 2020 shared with DFWG.

Safe, Secure and Prosperous: A Cyber Resilience Strategy for Scotland, Scottish Government, November 2015: https://www.gov.scot/publications/safe-secure-prosperous-cyber-resilience-strategy-scotland/

Scots paedo's huge stash of child images contained 'some of the worst' police had ever seen, Daily Record, March 2020: https://www.dailyrecord.co.uk/news/scottish-news/scots-peados-huge-stash-child-21680940

Scottish Biometrics Commissioner Bill, Scottish Parliament 2019: https://www.parliament.scot/parliamentarybusiness/Bills/111859.aspx

Scottish Government Serious Organised Crime Strategy, June 2015: https://www.gov.scot/publications/scotlands-serious-organised-crime-strategy/

Scottish Police Authority, Digital Forensics Working Group Terms of Reference, 26 June 2019: http://www.spa.police.uk/assets/126884/441011/509407/563684/item10a

SPA Corporate Governance Framework, 2018: http://www.spa.police.uk/assets/128635/293617/487394/488996

SPA Forensics 2026 Strategy, Scientific Excellence for Safer Communities: http://www.spa.police.uk/assets/126884/441011/441165/457127/item7.1i

SPA, Strategy Policy and Performance Committee report dated 8 May 2019

Strategic Review of Police Scotland's response to online child sexual abuse, HMICS, February 2020: https://www.hmics.scot/news/police-scotland's-response-online-child-sexual-abuse-reviewed

The Fingerprint Inquiry Scotland: Scottish Government, 2011 (Archived).

The Scientific Working Group on Digital Evidence (2019) www.swgde.org

UKAS, the route to accreditation, 2020: https://www.ukas.com/the-route-to-accreditation/