Forensic Science Regulator
Overseeing Quality

Quality Standards Specialist Group (QSSG)

Note of the meeting held on 13 November 2019 at Home Office, 2 Marsham Street, Westminster. SW1P 4DF

1. Welcome, Introduction and Apologies

1.1. The Chair welcomed all to the meeting. A full list of the attendee organisations and apologies is provided at Annex A.

2. Minutes and actions of the last QSSG meeting on 11 July 2019

2.1 The previous QSSG minutes were approved as an accurate reflection of the discussion held, subject to minor amendments, and the Secretariat was asked to publish them.

Action 1: The Secretariat to amend and publish the minutes of the QSSG meeting held on 11 July 2019 on GOV.UK.

2.2 The following matters arising from the previous QSSG meeting were discussed:

2.3 Action 1: FSRU to set up a working group to update the validation guidance. This action is currently in progress. The working group had been formed and would meet in early December.

2.4 Action 2: FSRU to examine Data Integrity audit cases that had been provided to FSRU by Forensic Science Providers (FSP) to see if a lesson learnt document could be developed. A 'lessons learnt' document had been produced and was awaiting publication.

2.5 Action 5: Eurofins Forensic Services representative to supply examples to be considered for inclusion in the expert report guidance. This action was ongoing.

2.6 All other actions were complete.

2.7 The following actions from the meeting of 11 July 2019 were discussed:

2.8 Action 1: The Regulator and the FSRU to circulate proposed guidance on IT security for comments and feedback. This action was complete

2.9 Action 2: Members to send any further comments on the Codes to the FSRU. This action would be discussed at item 5.

2.10 Action 3: FSRU to amend some of the wording under the summary of the general audit findings. This 'lessons learnt' document has been amended and this action was complete

2.11 Action 4: FSRU to investigate producing a webinar/video that informs individuals of the FSPs and CPS processes. This remains a focus for the FSRU but was removed as an action to be progressed at a later date.

2.12 Action 5: Discussion of audit of DNA consumables against ISO 18385. This action would be discussed at item 4.

2.13 Action 6: FRSU to set up a working group to look at Digital Forensic activities at crime scenes. This working had been formed and had met, this action was complete.

2.14 In addition, the group was informed that the response from the Regulator to the House of Lords report, that was discussed at item 7 of the meeting of 11 July 2019, had been published and the next step would be a debate in the House of Lords. This was awaiting return of parliament.

3. Cyber security consultation

3.1 The text for a proposed addition to the Codes on cyber security had been published on the Regulator's website for comment from the 6th of August to the 21st of October 2019. Comments from the website had been collated and provided to the group. The representative from the National Cyber Security Centre (NCSC) took the group through the main themes.

3.2 A recurring query in the comments was on self-certification and certification to other ISO standards. The NCSC was working with the National Police Chiefs' Council (NPCC) and the National Crime Agency (NCA) to better align their contractual requirements for cyber security as the requirement for Cyber Essentials plus (CE+) and ISO 27001 had come from the NCA. The NCSC as owners of the CE+ scheme did not make it mandatory for government. The NCSC representative commented that neither the CE+ or ISO 27001 standard added much value in addition to what was proposed for the codes and which would be assessed by UKAS. It was also noted that the scope and threat risk for CE+ was very specific and it didn't consider medium to large organisations or cloud-based storage.

3.3 The NCSC would look to work with UKAS to make sure their guidance can be assessed and can be interpreted; more detail and references may need to be added. The UKAS representative commented that it would be useful for the NCSC to liaise with their technical assessors.

Action 2: UKAS representative to liaise with the National Cyber Security Centre representative to ensure technical assessors have the information needed to assess against the cyber security addition to the Codes. The Regulator to share contact details.

3.4 There was also a query regarding the referencing of legal obligations as GDPR was referenced and the group considered that there were other legal obligations that would apply. It was agreed that the reference to GDPR should be removed as this was required elsewhere as well and there was a general comment to adhere to legal requirements. The

group also commented that if the standards were at the right level this would mean that the legal obligations were met.

Action 3: Remove the reference to GDPR from the proposed addition to the Codes on cyber security.

3.5 Feedback included a request for an explicit requirement for password length. The NCSC representative recommended three random words, these should be more than 8 characters in length.

3.6 Current password security controls included a three-attempt lock out rule and a 90-day password change rule, the representative from the NCSC stated that neither of these controls were based on any evidence of reducing security risk. The NCSC do not recommend passwords are changed unless there is suspicion that they were compromised, it was more important to manage accounts and know what they were being used for. In terms of a cyber-attack it was noted it would be rare to be observed entering a password and this used to attack. More commonly a cyber-attack would attack the site where the passwords are stored which will include the passwords for creating accounts.

3.7 The representative from the NCSC highlighted the importance of setting the right access for the right use for example, administrator accounts should only be used for completing administrative tasks, these were noted to be the easiest accounts to attack if they are used to browse the web, access email etc. Also, high sensitivity accounts should only be used for accessing sensitive data.

3.8 The representative from the NCSC recommended two security checks for log in.

3.9 The group commented some of the recommendations on passwords in the draft of the cyber security described as ‘should’, would be difficult to mandate. The representative from the NCSC stated that these requirements were strongly recommended, however the wording could be reviewed to ensure doesn’t prevent more stringent requirements that some users may have being followed.

Action 4: The representative from the NCSC to update the wording for the addition to the Codes to include a recommendation on password length and check that wording doesn’t prevent more stringent requirements that some users may have being followed.

3.10 The representative from Cambridgeshire Constabulary highlighted an issue with collaborative police forces and difficulty with changing IT. The representative from the NCSC commented that it would still be possible to carry out an audit of IT accounts, check accounts were still needed (staff still in post) and check the access privileges of accounts were still valid. Working closely with IT departments would be required.

3.11 The representative from SPA Forensic Services expressed concerns about support from the IT providers for Police Forces. The representative from NCSC suggested that it would help IT providers to be very specific with what was required of them.

3.12 The Regulator suggested that someone at the National Cyber Security Centre could write to the Police Forces, highlight the issues of cyber security and the requirements to move forward. The representative from the NCSC stated that this may be possible, and

members of the NCSC were colleagues working with senior City of London police officers on this.

Action 5: Representative from SPA Forensic Services to provide National Cyber Security Centre (NCSC) with contact details for the Head of IT at Police Scotland.

3.13 The representative from Orchid Cellmark commented that there was a risk of a two-tier system as private organisations would be expected to comply to security standards before police services. The regulator replied that the cyber security requirements would not be incorporated into version five of the codes, which are shortly to be released, it would be incorporated into version six. Everyone should be aware that the addition was coming which should mean that everyone would meet the requirement at the same time.

3.14 The group discussed the use and control of removable media. The representative from the NCSC stated that controls only needed to apply if the removable media was taken off-site. Data on removable media should be encrypted to be taken off-site and off-site use needs to be managed and logged. It was noted that not all devices needed to be able to use removable media and there should be controls on this. Also, removable media must be issued by the organisation, not personal, and must be scanned for malware immediately when it is connected to a computer. The addition to the codes does not require all removable media to be backed up but controls should be in place for how to recover lost data. The representative from the NCSC recommended alternatives to removable media, such as OneDrive and email as these were more secure than removable media.

3.15 The representative from the MPS asked how digital evidence should be dealt with where Police forces cannot scan for malware or encrypt because this would alter the evidence. The representative from the NCSC sought clarification on how the risk of malware was managed. This was achieved using a sandbox/separated system but clarity was needed on how these separated systems were protected so that malware from one exhibit didn’t corrupt the next exhibit.

Action 6: NCSC to liaise with Digital Forensics practitioners at the MPS, Cambridgeshire Constabulary, and Eurofins to establish what protections against malware are used when examining digital evidence and ensure codes reflect the specific requirement not to alter digital evidence.

3.16 The segregation of networks was discussed, flat networks make it easy for a cyber-attack to transfer from one area of business to another, as was seen in the Eurofins attack. Sensitive data and evidential data should be as separate as possible. In addition, the representative from the NCSC stated that the correct classification of network should be used for the work that was being done, sensitive forensic work and access to applications like email should not be done on the same desktop. Web browsers or email may introduce malware to forensic evidence if they run on the same systems. The representative from the MPS commented that this would be impractical, and this should be discussed further (see action 6).

3.17 The representative from the Expert Witness Institute commented that they would issue guidance to their members that laptops should be secured.

3.18 The group discussed remote working at crime scenes with laptops and remote transmission of marks from crime scenes. The representative from the NCSC stated that access controls would apply here and communications controls, would need to follow the guidance for cryptographic controls for transmission of data. The ideal situation would be to have controls on the laptop, for example second factor. There also should be controls on the databases that can be accessed remotely to ensure that the end user cannot access the full database, only the files they need.

3.19 The representative from Eurofins gave a summary of the issues faced from their ransomware attack. Segregation was highlighted as the key; digital forensics was not affected as it was on a segregated server. An ongoing issue was lack of awareness among staff on cyber security. Eurofins had launched a phishing campaign in-house to identify training needs and an internal and external penetration test.

3.20 The representative from the Chartered Society of Forensic Sciences asked if cyber security considerations were covered in computer forensic degrees. The NCSC representative commented that the NCSC accredits computer forensic courses and would expect cyber security to be a required aspect.

3.21 Considering teaching the NCSC representative commented that they had a knowledge exchange system where lessons learned could be shared and commented that a similar system for the forensic community would be helpful if this doesn't already exist.

4. Auditing suppliers of consumables against ISO 18385

4.1 Transforming Forensics was working with the representative from Orchid Cellmark to see if national batch testing of consumables for DNA contamination could be established by auditing manufacturers against their compliance of ISO 18385. The audit would check for evidence of a properly functioning QMS, measures to minimise contamination and maximise detection of contamination, properly functioning clean rooms and Ethylene Oxide gas (EtO) treatment and that consumables were protected from decontamination to delivery to the end user. The audit also looked at staff elimination databases.

4.2 An audit of a provider was carried out in the week before the meeting, the report of the audit could not be circulated as it was commercially sensitive. Processes were controlled and documented and the effectiveness of EtO treatment was tested. The representatives from Transforming Forensics and Orchid Cellmark commented that they found the audit valuable. The representative from Transforming Forensics asked the group if they would be content with the audit approach as a way to ensure independent assessment of consumable providers and whether auditing could replace local batch testing.

4.3 The representative from UKAS commented that it was great as a possibility if it gave greater confidence in the assurance of consumables and asked what the response by the company was to any actions raised in the audit. The representative from Transforming Forensics replied that the report was provided to the company and they would expect them to action all the issues raised before assurance could be confirmed.

4.4 There was discussion of the frequency of the audits, police national tenders for consumables ran on three-year contracts, if audits were repeated for every cycle would

this be frequent enough? The representative from UKAS commented that this was a different level of assurance to batch testing. Batch testing had identified issues that were not picked up by manufacturer processes. A representative from the FSRU suggested that some level of batch testing could be carried out to ensure that the manufacturers were meeting their requirements. The representative from Transforming Forensics commented that end users would be able to access company data on EtO.

4.5 The group commented that the risk of not identifying contamination was too great if relying on someone else's audit where the findings and actions raised in the audit were not seen by the end user and that the time periods were long which would mean a lot of reinvestigation if something was picked up. The representatives from Transforming Forensics and Orchid Cellmark agreed that batch testing was not going to determine if a batch was free from sporadic contamination, however they thought that the audit and validation of the process would provide more assurance than batch testing.

4.6 The representatives from Transforming Forensics and Orchid Cellmark explained that to check EtO success the manufacturer spiked each batch with DNA and they were required to show a 10,000 fold reduction in DNA levels. A representative from the FSRU commented that batch testing could be seen as investigating contamination after EtO. The representative from Transforming Forensics replied that this was well protected against and stated that batch testing would pick up gross contamination, failure of EtO, therefore if validation of manufacturers proves that contaminated consumables would not reach an end user then batch testing would not be needed.

4.7 The group asked about validation of the manufacturer's batch testing process. The representative from Transforming Forensics replied that they hadn't seen the validation data as this would require a non-disclosure agreement which was in progress. The representative further commented that the data that was provided with each batch would give the assurance that end users need. This data gave information on the reduction of DNA levels in the spiked samples.

4.8 The representative from Transforming Forensics also commented that the consumables packaging was sensitive to EtO treatment and showed that the treatment had been successful. The representative from UKAS asked what amount of EtO gas was required to change the colour of the packaging and whether this was equal to the amount required to denature the DNA in the consumables.

4.9 The representative from Eurofins suggested that the group establish what assurance was required to remove the requirement to batch test. The representative from Transforming Forensics commented that reports could be sent out to all the FSPs and police forces.

Action 7: The representatives from Transforming Forensics and Orchid Cellmark to review the validation documents from the consumables manufacturer that they have audited and create a document setting out what would be required to seize batch testing by end users.

4.10 The representative from UKAS commented that there was still a need to address the assurance at point of use in terms of protection from contamination. The representative from the CSFS added that there is also a need to ensure that CSIs understand the risks of introducing contamination.

5. Codes

5.1 A draft update of the Codes of Practise and Conduct was circulated to members. This document was still in development.

5.2 A code of practice on gait analysis will be out this month.

5.3 The group was asked for comments on the firearms section of the codes and to review and comment on changes to the codes document.

5.4 The representative from UKAS requested that the term complainant be defined. The term patient was now being used in the medical forensics guidance. The UKAS representative also requested that a prompt for reviewing validation work be added.

5.5 The representative from Orchid Cellmark commented that points f) and m) on page 23 were repetitive and could be combined.

Action 8: FSRU to make the following amendments to version 5 of the codes; add a prompt on review and update of validation; merge f) and m) on page 23; define the term complainant.

5.6 A representative from the FSRU highlighted that the Medical Forensics requirements will be in the new codes so the Medical Forensics Guidance document needed to be published shortly after the codes and if the members had any comments on this document, they should be submitted to the FSRU as soon as possible.

5.7 The group were informed that cyber security requirements would be included in a further update to the codes but that the FSRU would ensure that this doesn't follow to closely after Version five.

6. Proficiency Testing Guidance for DNA Mixture Analysis and Interpretation

6.1 The group was provided with a draft of FSR-G-224: Proficiency Testing Guidance for DNA Mixture Analysis and Interpretation. This document included learning from the collaboration with FSPs on mixtures interpretation which also resulted in a guidance document on processing and interpretation. These documents can be taken independently, for example in a case review where only interpretation is carried out.

6.2 The FSR's DNA specialist group has reviewed this guidance document and commented that there was an issue with the volume of data produced and the complexity of interpretation. The FRSU representative wanted to ratify this document at the DNA SG meeting in the next week and requested that any feedback on the document be returned to the FRSU by 27/11/19.

Action 9: Group to provide comment on the Proficiency Testing Guidance for DNA Mixture Analysis and Interpretation by 27/11/19.

7. Medical Forensics

7.1 The Regulator introduced this item, explained the remit of FSR in this area and that the forensic element of Sexual Assault Referral Centres (SARCs) was a small aspect of their job. The Care Quality Commission (CQC) had started inspecting SARCs but were avoiding any forensic aspects. The group were informed that workshops would be running over the next few weeks with the CQC, the NHS and the FSRU to be clear on roles and requirements, as SARCs were all set up in different ways this would be complex.

7.2 The Regulator commented that it would subsequently be necessary to look at medical examinations in custody.

7.3 The Regulator asked for input from this group on this standards document and this group was more familiar with quality standards. As the accompanying guidance document was large the Regulator asked the group to concentrate review on the standard but refer to the guidance document if needed. The group were asked to return feedback to the FSRU by the end of November.

7.4 The representative from the MPS asked for clarity on who the standards document applied to. The representative from the FSRU replied that this was for any patient requiring medical examination as a result of an alleged sexual offence, it couldn't apply to historic examinations or examinations in A&E and it did not apply to suspects. The representative from the MPS suggested that the current wording suggests all medical examinations of a sexual assault patient not just intimate examinations.

Action 10: Members to provide comment on the Standards and Guidance for Forensic Medical Examination of Adult and Child Sexual Assault Patients by 29/11/19.

Action 11: The representative from the MPS asked for clarification of the scope of the Medical Forensics Standard in that examinations refers intimate examinations and not other medical examination unrelated to the alleged sexual offence.

8. AOB

8.1 The FSR response to the Forensic Science Synergy paper on image analysis has been published.

8.2 The Digital Forensics group had been reviewing standards and a paper should be submitted tomorrow to FSI – Digital Data.

Date of next meeting:

The next QSSG meeting will be held on Monday 16th March 2020.

Annex A

Organisation Representatives Present:

- Forensic Science Regulator (chair)
- Forensic Science Regulation Unit
- Chartered Society of Forensic Sciences
- Eurofins Forensic Services
- Expert Witness Institute
- Forensic Science Northern Ireland
- HO Science Secretariat
- Key Forensic Services
- Metropolitan Police Service
- Cambridgeshire Constabulary
- National Cyber Security Centre
- National Quality Managers' Group
- NPCC Portfolio
- Orchid Cellmark Ltd
- Scottish Police Authority Forensic Services
- Transforming Forensics
- United Kingdom Accreditation Service

Apologies:

- College of Policing
- Criminal Bar Association
- Crown Prosecution Service
- Defence Science and Technology Laboratory
- Glaisyers Solicitors Birmingham
- Legal Aid Agency
- Manchester Coroner's Office
- National Crime Agency