OSC/INSP/219

[redacted]
Investigatory Powers Commissioner
Investigatory Powers Commissioner's Office
PO Box 29105
London
SW1V 1ZU

28th September 2018

IPCO INSPECTION – POLICE SCOTLAND

1 Date of inspection

17th to 21st September 2018.

2 Commissioner and date of visit

You will visit the Force on a date to be advised.

3 Inspectors

[redacted]

4 Introduction

4.1 Police Scotland was formally established on 1st April 2013 and is responsible for policing across the length and breadth of Scotland, covering some 28,168 square miles. The Force has 17,234 police officers, 4,928 police staff, and 550 Special Constables who work alongside their full time colleagues to deliver the policing service to the public of Scotland. The force remains the second largest Force in the UK after the Metropolitan Police Service.

4.2 The senior management team has seen significant change since the last inspection but it is hoped there will now follow a period of stability. The Chief Constable is Mr Iain Livingstone QPM, who was previously the Deputy Chief Constable and latterly temporary Chief Constable. Mr Livingstone was appointed to the substantive rank on the 27th of August 2018. He is supported by a team of three Deputy Chief Constables. Deputy Chief Constable Fiona Taylor was appointed to the role in August 2018 and oversees the Professionalism portfolio for the Force. In addition DCC Taylor performs the role of Senior Authorising Officer (SAO) in the absence of Mr Livingstone. Deputy Chief Constable Will Kerr, OBE leads the Local Policing Portfolio and was appointed to the Force in September 2018. Deputy Chief Constable Johnny Gwynne, QPM has been in post since the last inspection and leads the Crime and Operational Support portfolio. DCC Gwynne is also the Senior Responsible Officer (SRO) for the Force for matters concerning the Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A).

4.3 The Chief Constable is further supported by ten Assistant Chief Constables (an increase from eight since the last inspection) and four Directors (an increase of one since the last inspection), each covering the areas of People & Development, ICT, Business Integration and Change).

4.4 The force remains divided into three Territorial Control Areas: North, East and West, which cover thirteen Local Policing Divisions, each of which is led by a Local Police Commander. Each of these Divisions has response officers; community officers; local crime investigation; roads policing; public protection; and local intelligence.

4.5 The Force has retained its six specialist divisions: Contact Command & Control; Custody; Criminal Justice; Safer Communities; Operational Support; and Specialist Crime Division (SCD). The SCD houses the main business areas with which the IPCO inspection is concerned: Major Crime, Public Protection, Intelligence Support, Organised Crime and Counter Terrorism and Safer Communities. Detective Superintendents within the Public Protection and Crime roles provide additional support to local police commanders by managing resources and incidents connected to crime, intelligence and public protection within the divisions.

4.6 The Senior Responsible Officer, DCC Johnny Gwynne (Crime and Operational Support) was interviewed during the inspection in order to ascertain how he discharges these additional duties. ACC Steve Johnson, lead for Crime, was also spoken to at length concerning his role as AO for "Relevant Sources".

4.7 This report should be addressed to The Chief Constable, Police Scotland, Tulliallan Castle, Kincardine, Fife, FK10 4BE [redacted]

5 Inspection approach

5.1 The purpose of the inspection was to examine policies, procedures and operations in respect of Part III of the Police Act 1997, Part II of the Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A) and Part III of RIPA. The methodology was agreed with the Force in advance following pre-inspection discussions between [redacted] and the CAB Manager, [redacted] A significant amount of time during this inspection was focused on CHIS cases and a direct result of the recommendation made in last year's report concerning the need for fuller risk assessments to be completed. In addition it was recognised that there was a complex nature to many of the CHIS cases undertaken by the Force. Meetings with officers took place at Gartcosh and at outlying locations. In addition, IPCO Chief Inspector, [redacted], spent two days in Aberdeen, reviewing the CAB procedures, inspecting directed surveillance authorisations and CHIS cases as well as interviewing staff from these disciplines. The findings from this visit and other visits to divisional units, which support these covert tactics, have been reported on within the report under the relevant headings of CHIS and directed surveillance. The main inspection team was also shadowed, for part of the week, by one recently appointed IPCO Inspector and a member of the IPCO staff charged with a review and potential development of inspection practices.

5.2 On the third day of the inspection, Wednesday, a further five Inspectors from IPCO, involved in the inspection of Communications Data, joined this inspection team in order to carry out a more holistic inspection of a major covert operation (Operation [redacted] This operation has been progressing for a number of years and has more recently seen executive action take place, with a number of individuals already convicted for their criminal enterprises. A number of further investigative lines are still being pursued. It is without doubt that this operation was complex with

unique challenges faced by the investigation team who were supported through the development of a wide range of covert tactics. The inspection team received an in-depth briefing from the SIO for the investigation who was able to answer questions posed by the inspection team prior to the inspection of the associated covert authorisations. Feedback on the standard of the full range of authorisations examined and feedback on the inspection process was given and received at the end of the day. We would like to thank the SIO [redacted] and the CAB manager for their significant efforts in planning this inspection day.

6 Key statistics

6.1 In the period covering 5th September 2017 to 13th September 2018 there have been [redacted] property interference authorisations ([redacted] the last reporting period); one for intrusive surveillance with a further [redacted] authorisations for combined Property Interference and Intrusive Surveillance ([redacted] in the last reporting period); [redacted] directed surveillance authorisations ([redacted] last time); and at the time of the inspection, there were [redacted] (compared to [redacted]) authorised CHIS, with [redacted] (down from [redacted]) for Counter Terrorism. There have been [redacted] undercover operatives authorised. [redacted] Part III RIPA (section 49 Notices) have been sought [redacted] successful conviction, the first time this has occurred in Scotland, has been achieved for a case which was highlighted within the previous inspection period.

6.2 During the course of the inspection, the following records were viewed:

- 17 directed surveillance authorisations [redacted]
- [redacted] property interference and intrusive surveillance authorisations (including [redacted] urgent oral authorisations)
- [redacted] crime, Prison and Counter Terrorism CHIS records
- [redacted] undercover operations

7 Review of progress on recommendations

7.1 *In relation to directed surveillance*:

When granting directed surveillance under the urgency provisions, Police Scotland should ensure that both the Authorising Officer and the applicant make a record detailing the specific actions authorised in accordance with paragraph 3.26 and 5.10 of the Scottish Code of Practice for covert surveillance.

Discharged. A notable improvement was discovered, when documenting the activity authorised during the urgent oral process by both the AO and the applicant and thus leaving no doubt as to the exact activity authorised as well as any parameters set therein. That said, further comment is contained later in this report with regards to the volume of content now contained within these records (see paragraph 12.4 below). The improvement in the details documented during the urgent oral process is believed to be largely due to the training and education process put in place by officers from the Central Authorities Bureau (CAB). It was noted that awareness training was delivered at a number of Continuous Professional Development (CPD) days held for Senior Investigating Officers (SIOs), AOs and those involved in the investigation of dynamic, serious crimes such as kidnap and extortion. In addition the training and awareness programme has been embedded within initial training for SIOs, newly appointed Sergeants and those training to act as RIP(S)A gatekeepers. The Force training guides have been updated with a focus placed on the

need for applicants to understand exactly what has been authorised, as opposed to what they may have requested, and further emphasis placed on those deploying the tactic to have sight of the authorisation thus complying with the *R v Sutherland* requirements.

7.2 *In relation to CHIS*:

Initial risk assessments should always provide a meaningful and bespoke summary of the individual CHIS, to enable the Authorising Officer to make a reasoned judgement before authorisation, and the force should ensure that all Source Handling Units adopt a corporate approach to such content. With the introduction of the generic ongoing risk assessment, the force should determine a set period (in routine cases) at which there should be a meaningful and documented revisit of the risk assessment for any authorised CHIS.

Discharged. A thematic review of CHIS risk assessments was undertaken with best practice examples used to form a training delivery package. CPD events were held with those involved in CHIS authorisation and management. The emphasis was placed on delivery of a corporate approach with a similar standard of assessment conducted for each CHIS case. Additionally a 13 point risk assessment questionnaire has been developed which should be completed by the CHIS handling team at the earliest opportunity and after intrusive engagement with the CHIS has taken place. It was also reported that once a risk is identified, the advice and guidance now in place, is for the risk assessment to be updated promptly, with the AO then having access to a newly developed "rolling log" which should make clear the continuing risks associated with the CHIS case. It was noted during the inspection of CHIS cases, particularly during the inspection of cases in Aberdeen, that there was a significant reliance on the generic risk assessment. Whilst this is normal practice, with specific risks additionally highlighted, it was noted that the generic risk assessment is circa two years old. It may be beneficial to review the generic risk assessments used by the Force to ensure they continue to be relevant in what is an ever changing CHIS management environment. Review of the risks posed to CHIS and the management of same has been undertaken with a recent audit of the Counter Terrorism CHIS 'stable'. This included personal and intrusive oversight undertaken by ACC Johnson. It was reported that a further, similar review, will be conducted within the crime CHIS 'stable' in the near future.

8 Policies and procedures

8.1 The force's covert capabilities have not changed materially over the past year but oversight arrangements have changed with the introduction of two newly appointed AOs to the cadre which numbers [redacted] in total. Additionally the CAB has seen some change due to the retirement of the CAB manager and the introduction of a number of new RIP(S)A gatekeepers. The new CAB manager and some of the newly appointed staff have previous covert policing experience and continue to develop compliance with the Act through daily advice and guidance and an improved and extensive training delivery programme.

8.2 A briefing was provided by Detective Chief Superintendent [redacted], head of the Specialist Crime Division and Intelligence Support, on the recent and proposed changes within the areas of CHIS (referred to by the Force as "Human Collections"), Covert Policing Support, Central Authorities Bureau (CAB), Authorisation and National Intelligence Assessment Unit. These changes can be summarised as follows:

i. Human Collections Review – Changes in the CHIS operating model were identified as required following an internal review of the legacy structures, in place since the formation of Police Scotland, and additionally following the judgement of the Court of Appeal regarding *Allard & Ors v Chief Constable of Devon and Cornwall Constabulary*. As a result a significant number of changes in CHIS handling and management structures will likely take place with a number of CHIS handling teams or Dedicated Source Units (DSUs) being formed into larger 'hubs', working from single offices. Some of the identified benefits are likely to be an improvement in delivery of CHIS intelligence across the organisation, consistency in CHIS handling and management, the provision of an equitable service across Police Scotland, and an improved ability to service the intelligence requirements of the Force. It is anticipated that the revised structures will be in place by January 2019.

ii. Covert Policing Support Unit – A significant investment has been undertaken in the area of support for covert policing. This has included the development of staff, processes and procedures in order to support covert policing operations, the delivery of covert tactics, the administration of covert equipment purchases and wider covert support mechanisms in order to sustain and protect sensitive covert techniques and those officers delivering these. The unit was visited during the inspection. Further details are contained within paragraph 22.3.

iii. National Intelligence Assessment Unit – The (NIAU) has continued to evolve and following a theme of developing a more authoritative view of intelligence across Police Scotland in order to identify and assess the threats emerging within Scotland and beyond. The unit is staffed by officers and staff 'plucked' from a variety of key roles including CHIS management, financial crime investigation and those involved in the management of various intelligence products. The collective benefit of the unit is the ability to identify threats and cross reference these with the identified policing priorities, adopted by the Force. The unit was visited during the inspection and is reported upon at paragraph 15 of this report.

iv. Central Authorities Bureau – Currently three CABs exist to service the Force by acting as professional applicants for higher level authorisations, RIP(S)A gatekeepers, and to offer advice, training and guidance regarding matters relating to RIP(S)A and the forthcoming Investigatory Powers Act 2016 (IP Act 2016). The proposed changes are anticipated to take place in January 2019 and would see one single CAB, [redacted], being strengthened but with the closure of the offices currently located at [redacted]. It was reported that the drivers for these changes include the availability of current operating systems required to deliver the implementation of the IP Act, a business need to increase CAB coverage across the working day and the potential to improve security requirements. Some of the potential benefits of the proposed changes have been identified as business continuity, additional flexibility of staff to assist each other and the ability for CAB staff to increase upskilling opportunities for staff across the Force. That said, during the inspection of the CAB located in [redacted], concern was voiced as to the potential affect closure of this office would have on the quality of applications and authorisations post closure. Whilst the force structure and allocation of resources is beyond the scope of IPCO's remit, it would be amiss not to highlight the impact this locally based CAB appears to have on the quality assurance process for directed surveillance, and in particular, the work of three dedicated source units running CHIS. This was clearly evidenced by the high standard of the records inspected and it was also evident during the visit through the constant stream of calls and visits to the CAB from applicants, managers and the authorising officer, that the experienced staff in this CAB fulfil more than just a process function and operate more akin to a covert advice help desk. It may well be these factors have already been taken into consideration in the restructure arrangements but the observation is offered just in case it has not been previously highlighted.

8.3 The [redacted] IT system continues to be used for the authorisation and Central Record processes for all covert activities. Property interference and intrusive surveillance authorisations are still managed on paper for a final signature and handwritten annotation by the SAO. It was reported during the last inspection that funding had been agreed to allow the IT systems to be upgraded. This included the introduction of a new module for the management of undercover cases. It was reported that in February 2018 a new upgrade for the IT systems, commonly referred to as [redacted], was undertaken. A number of technical issues occurred during this process which has in turn led to a delay in the testing and further installation of additional modules, such as the undercover case management module. It is anticipated that the systems upgrade will take place within the near future and the undercover module, which is recognised as much needed, will be introduced within the next few weeks. It was reported that during the period when technical issues were occurring, Police Scotland was required to introduce its business continuity plan to ensure no issues of record deletion occurred for CHIS authorisations. Whilst no compliance matters were noted due to the lack of progress in the updating of the IT systems, it was clearly evident during the inspection of areas such as the undercover policy logs that a confusing picture existed regarding the individual logs retained for each undercover operative. This in itself could lead to future compliance matters if not attended to promptly.

8.4 The Force has recently announced that the number of Operational Security Advisors (OpSys) will be increased. At present one OpSy is in post. This officer has been exemplary in his development of new covert practices within the Force as well as undertaking a number of operational reviews post event and by providing advice and guidance during operational development phases. It is without doubt that the officer's dedication to the development of strategic practices, which will benefit the Force, was and continues to be required but it is hoped that the 'uplift' of resources in what is now recognised as a critical role, will further assist the Force in the review of more tactical aspects of covert policing. Further details of the proposed OpSy structures are reported upon later in this report at paragraph 8.6.

Senior Responsible Officer [redacted]

8.5 The Senior Responsible Officer is DCC Johnny Gwynne. In order to maintain corporate grip of the covert activities in Police Scotland, DCC Gwynne has developed a number of initiatives. First, the core purpose of the Covert Compliance Group, chaired by ACC Johnson, is scrutiny of compliance in relation to the full range of covert activities across the police force. This group provides the SRO with an effective mechanism to keep in touch with these activities and ensure compliance with RIP(S)A, Part III of the Police Act 1997 and the Codes of Practice. DCC Gwynne attends some meetings, receives the minutes of all and has regular meetings with ACC Johnson. Second, DCC Gwynne has presided over a complete revamp of covert finances and backstopping. This has resulted in a state-of-the-art scheme which has been validated by the banks and is operationally secure. Third, the role of Operational Security Officer (OpSy) is being strengthened and expanded as alluded to previously. With these structures in place the SRO has a good appreciation of corporate risk and is in a position to check and challenge processes.

Operational Security [redacted]

8.6 It was reported in the 2017 inspection that additional posts, to support the Detective Chief Inspector who had been appointed as the OpSy, had been approved. Whilst no substantive progress has been made in this regard, an even more elaborate 'Covert Governance and Compliance' structure has been approved. This will come under the strategic leadership of the ACC (Crime) and be headed by a Detective Chief Inspector (Head of Operational Risk). There will

be three OpSy officers each with a portfolio of responsibilities, comprising specialist support functions/units. Each of these functions/units will have an appointed and trained Operational Security Liaison Officer (OSLO) who will give advice in situ and be the point of contact for their OpSy. In addition there will be two Detective Sergeants who will undertake inspections and reviews, predominantly of CHIS and surveillance. The above cited model is innovative, intrusive and comprehensive. It just needs implementing, rather than IPCO speaking about what is planned at our next inspection. That said, the sole current practitioner in this aspired to model has achieved much more than just setting out the model and agreeing a Role Description for the post of OpSy that has been adopted on a national basis (a real step forward for what has hitherto been a rather nebulous role among law enforcement agencies). In addition the officer has carried out several important audits into covert support infrastructure. One such audit has led to the creation of the Covert Policing Support Unit.

9 Related training

9.1 We were provided with a comprehensive report on the Force investment into training its officers since the last inspection. The officers from the CAB office have been instrumental in the development of training. It was reported that a total of [redacted] officers have been trained since the last inspection. These officers originate from a wide range of policing backgrounds, such as firearms teams, intelligence departments and also those charged with the authorisation of covert tactics up to and including DCC Taylor, who performs the role of SAO in the absence of the Chief Constable. Following the last inspection the Force AO cadre received refresher training and the urgent oral authorisation process, subject of a previous recommendation, was the topic focused upon. The training delivered for authorisation of the urgent oral process and the standard of documentation required was emphasised in training sessions delivered to those investigating kidnap and extortion cases, those attending initial training as newly promoted sergeants, and SIO induction courses. In addition to the training delivered to assist with the discharging of the previous recommendation, a number of other areas were identified as needing further training and refresher inputs. These areas referred to are the development of the standard of undercover applications; development of force wide guidance on the use of the internet for investigation purposes; Technical Support presentations to the AO cadre and SAOs; and CPD events at three locations across the Force where a variety of topics were discussed including the use of policy logs, review periods for authorisations and the standards expected when applying for directed surveillance authorisations. Additionally a number of post operation reviews have been carried out to identify learning points and to ascertain if there had been a proportionate use of covert tactics. The Force continues to invest heavily in training within these covert policing areas which is seen as continuing good practice.

9.2 The main CAB office, led by [redacted] has also continued to develop professional relationships with other Law Enforcement Agencies as part of the working group in respect of the IP Act. This has allowed the Force to be on the 'front foot' in terms of the training and education of its officers and also in terms of putting in place the additional infrastructures deemed required.

10 Significant issues arising

Breaches/Errors [redacted]

10.1 The details of three breaches reported to the Investigatory Powers Commissioner (IPC) during the past year were provided to us. [redacted]

[redacted]

10.2 In all of these notified cases, the limits of the authorisation should have been identified through a check of the authorisation prior to deployment. Each breach was avoidable had the officers ordering or conducting the surveillance checked that the necessary authorisations were in place. [redacted] The IPC was satisfied with the remedial action taken by the Force in each of the three breaches/errors reported.

Confidential information

10.3 The force reported no case in which confidential information has been obtained and we found none during our inspection sampling.

Encryption [redacted]

10.4 [redacted] applications have been made under Section 49 RIPA to access encrypted material during this inspection period. One previous application, made in 2017, has since seen the [redacted] successful prosecution within Scotland, for failure to disclose password access.

10.5 We were invited to comment on a proposed pro forma to be used in relation to requests for passwords, PINs etc where a device is seized. This is against the background of potential applications under section 49 RIPA. We discussed the proposal with [redacted], interim Head of Legal Services. Typically, a request for a password is made at or around the time when a device is seized. Where the person to whom the request is made refuses to disclose the password, an application may be made in terms of section 49 for an order requiring the person to disclose it. Where a person is in breach of such a requirement a prosecution may follow. The concern is that by the stage of the section 49 requirement the person may claim that he/she is no longer able to remember the password. The proposed pro forma records the making of the request at the time when it is made and contains the following statement: *"As you have refused to provide [key/password/PIN/biometrics] for the device/s being seized, Police Scotland advises that you record these details to comply with any future legislative request that may be made."* It is clear that the pro forma contains non-statutory advice which, it is hoped, might have evidential value in any subsequent trial. While the service of non-statutory documents by officers of Police Scotland is unusual, it is not entirely unknown. While noting the proposal, we came to the conclusion that it would be inappropriate for the representatives of IPCO to express a view about it. Whether to adopt this practice is a decision to be made by the Chief Constable with internal legal advice.

11 Property interference and intrusive surveillance [redacted]

11.1 We examined a number of authorisations granted by DCC Livingstone (as he then was) and DCC Rose Fitzpatrick. These were granted in the context of a range of criminal investigations including several into significant OCGs. It was noted in last year's report that an OCG based in Scotland was ranked among the most, if not top, high risk/damaging to the UK. In the past 12 months there have been successful prosecutions arising from this operation and the investigation continues. The standard of the higher level authorisations continues to be very high. Applications were generally well drafted with clearly focused necessity and proportionality cases. We noted that regular reviews were conducted and, where use of the covert measure was no longer necessary or appropriate, authorisations were promptly cancelled. In a cross-border case we noted that there was a good audit trail of the actions taken by each of Police Scotland and the neighbouring force.

12 Directed surveillance [redacted]

12.1 I inspected a selection of authorisations from a variety of Divisions and headquarters teams, finding that covert tactics had been applied to a broad range of investigations including drugs, organised crime, murder, prison corruption, registered sex offenders, firearms, child abuse, and infant death. The applications and authorisations had been compiled carefully, with due regard to the key issues of necessity and proportionality. Intelligence cases were generally detailed (arguably capable of being less prolix at times) showing the recentness and grading of the material. Reviews were undertaken at an appropriate stage, depending on the activity and need for enhanced oversight, and it was good to see that all had been cancelled timeously.

12.2 There were no systemic compliance failings. A number of positive observations could be made in individual cases, and similarly, points meriting attention. These are mentioned here to better inform supervisors and future training material:

i. Whilst not a statutory requirement, there had been some very pertinent entries by [redacted] (the SIO) at the application and review stage of Operation [redacted]

ii. The cancellation statement in [redacted] provided a neat summation of the various aspects an Authorising Officer should comment upon at cessation.

iii. [redacted] involved surveillance on a very high profile sex offender who had been unexpectedly released from a trial that morning involving a very serious crime – despite the pressure to maintain knowledge of his whereabouts and actions, this was completed as a routine, albeit speedy, authorisation instead of resorting to the urgent oral process, which reflected the confidence of officers and the processes in place to achieve this promptly.

iv. The proportionality arguments by the applicants in [redacted] (at its first review stage) and in [redacted] were lacking specificity; in the latter case, all that was requested was some surveillance to house a suspect prior to arrest, yet the proportionality argument provided a blow by blow account of a historic case and the DNA evidence trail over ensuing years – this could have been a single background sentence.

v. Collateral intrusion entries varied, and only occasionally was there a case that felt truly bespoke to the case in hand (see the application for [redacted] for a good example, and which contrasted starkly with the subsequent necessity and proportionality arguments by the Authorising Officer). Whilst most cases appeared to justify the request for, and grant of, a range of tactics, or would quickly develop to need them, in some cases this appeared less likely and could have been more tightly drawn. For example, in [redacted], the cancellation suggested that the likely location of the wanted subject was known and enabled a very short period of surveillance before arrest (and thus the various other tactics were probably uncalled for at the outset); in [redacted] it was difficult to see how surveillance beyond the Scottish border was justified.

vi. At reviews, the [redacted] form asks the applicant to state the activity to which the review relates. It would be better practice to summarise the activity authorised at each stage (where subjects have been removed or added at other reviews for example) rather than merely regurgitating the original authorisation wording until a revamp at the renewal stage; and the Force is encouraged to make use of Policy Logs or suitable contemporaneous records to make subtle changes instead of the full-blown reviews sometimes submitted.

12.3 [redacted]

Urgent Oral Applications [redacted]

12.4 Police Scotland has adopted the use of booklets when completing urgent oral authorisations. The booklets should be completed at the time of the authorisation by the Authorising Officer and supported by the submission of the applicant's contemporaneous notes. A subsequent application is placed on [redacted] to enable the authorisation to be managed as it progresses. The booklets are designed to capture the Authorising Officer's thoughts and considerations in a concise and contemporaneous manner in an effort to support what is an urgent process. With regard to those completed for directed surveillance, over half were inspected. The majority contained far too much information. Authorising Officers are generally writing far too much and while this is not a compliance issue, one does start to question whether the urgency process is the right one. There are a number of examples that support this observation. The authorisation for [redacted] contains a full account of the intelligence case detailing fully the content of nine intelligence logs, making it incredibly long. The same authorisation contains unnecessary and repeated detail in what should be a simple and easy to understand list of activity

authorised. The authorisation for [redacted] is another relevant example where the authorisation section has required extra pages. The authorisation for Operation [redacted] is excellent and could be used as an example of good practice for others. There is also some helpful guidance contained within paragraphs 5.8 to 5.10 of the current RIP(S)A Surveillance and Property Interference Code of Practice.

13 CHIS [redacted]

13.1 Police Scotland uses the [redacted] IT system for the management of covert human intelligence sources (CHIS) reporting on crime matters. The system is fully networked throughout the Force albeit that authorising officers, controllers and handlers can only view those CHIS in which they have a role. The CAB carries out corporate oversight and can view all CHIS cases.

13.2 The Counter Terrorism (CT) cases are managed on a discrete [redacted] network. There is consideration being given to changing to the Security Service, [redacted] IT system. [redacted]

13.3 The cadre of [redacted] authorising officers carry out this role in relation to CHIS on a geographical basis with some specialism in relation to Counter Terrorism and CHIS in prisons. The following units have responsibility for the handling and recruiting of CHIS:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

13.4 [redacted] Detective Chief Inspectors divide the aforementioned units between them and have responsibility for the performance of those units, ensuring that intelligence product addresses the Force strategic intelligence requirements, local policing requirements and for ongoing liaison with customers and attendance at tasking meetings. Monthly performance indicators are produced in this regard.

13.5 During the course of the inspection a number of SHU were visited, controllers and authorising officers were interviewed and [redacted] CHIS cases examined (crime and CT).

Crime CHIS

13.6 Overall, the standard of authorisations was good. Records were comprehensive, Risk Assessments were thorough and dynamically maintained, there was good use made of the Policy Log facility to record management decisions. There was no evidence that 'status drift' was being allowed to occur and timeliness of process was maintained.

13.7 Whilst there were no systemic failings or flaws the following points for improvement should be noted:

i. Notwithstanding the Force's substantial response to the previous recommendation in relation to Risk Assessments for CHIS, there were some isolated cases where this had not yet been fully implemented. We were made aware by some authorising officers that there was resistance among some handlers to the new Risk Assessment regime, in particular the introduction of the Vulnerability Assessment. Controllers should ensure that such resistance is eradicated to ensure that IPCO does not need to raise this as an issue in future inspections.

ii. The input from authorising officers demonstrated good consideration of the required key principles and a good awareness of case specific risks; however, while some set out their input in a clearly structured way with sections relating to necessity, proportionality, collateral intrusion and then the use and conduct authorised, with others this was not done and it was difficult to discern the relevant considerations in a unstructured and lengthy input. This is not a compliance issue but the former style is better practice.

iii. There was some evidence in CHIS cases [redacted] in [redacted] and [redacted] Division that tradecraft/security following meetings with CHIS was not fully considered and recorded on contact records. [redacted]

13.8 The inspection team fully accept that the authorising officer cadre has undergone major change in the past year with three officers having retired and further change is to happen in the next few months with the further loss of experience. Nevertheless, the incumbents must exercise robust governance of the CHIS cases for which they are responsible and the staff managing those cases. Some of the individual cases that are cited below gave some concern that this is not always happening. Whilst each has given cause for some concern, there is not a systemic or repeated failing, which would have resulted in a formal recommendation, but we feel that the Senior Responsible Officer should be aware of the facts that gave rise to our concern.

13.9 [redacted] The record is generally well maintained and applications, reviews and authorisations contained all that is required. The later entries in the record show reluctance on behalf of the CHIS to engage with handlers. [redacted]. Once identified by Inspectors the matter was raised directly with the authorising officer who confirmed he had not been made aware of recent events and agreed that an immediate review was required.

13.10 [redacted] – [redacted] The initial authorisation for use and conduct was granted by an authorising officer on the [redacted] On the [redacted] the first review of the authorisation was undertaken by another authorising officer. It was established that the authorising officer for the CHIS case is the latter officer and that the initial use and conduct authorisation was only granted by the former due to the latter being on leave at that time. I did not note anything within the associated CHIS documentation to state this, neither did I observe anything to indicate that a handover brief had taken place nor that the clear lines of authorisation required, in what is a high risk case, had been communicated to the handling team. Matters such as a change in authorising officer and a handover brief would be expected to have been documented, mostly likely within the CHIS policy log.

13.11 It was noted within the risk assessment for the CHIS that the list of [redacted] Vulnerability Assessment questions, developed by Police Scotland for the purposes of better assessing risk factors, had not been discussed with the CHIS. It could not be established from reading the associated documentation and in particular the CHIS policy logs, why this was the case and why the authorising officer had not been more intrusive into why these risk factors had not been assessed.

13.12 [redacted]

13.13 Within contact note [redacted] it was noted that the CHIS had supplied intelligence which related to a potential serious crime being planned by a named individual. Recognising the sensitive nature of the reporting, a decision was made to sanitise the full intelligence report before disseminating this further. Whilst this is a recognised and required procedure, I noted that on this occasion the controller had decided what intelligence to disseminate and what not to disseminate. There was no indication that the authorising officer had been made aware of this nor was there any indication of when a review of the remainder of the intelligence would take place in order to ascertain when, if at all, the further intelligence could be disseminated. Whilst I recognise that the controller is responsible for the day to day management of the CHIS case, the authorising officer should ensure that they are sighted and included in any major CHIS management decisions.

13.14 [redacted] – [redacted] This CHIS was recruited as someone who could provide intelligence on cyber crime and in particular those who were carrying out cyber attacks. Authorisation was granted on [redacted]. Within a short time of authorisation the CHIS was reporting that there may be an attempt to hack the [redacted]

[redacted]

13.16 [redacted] In the previous inspection of Police Scotland I was asked to review this case as the authorising officer (who has now retired) had some concerns regarding it. In summary the CHIS was reporting on the main subjects of an investigation into the [redacted] The Force was desirous to retain the CHIS coverage, as the sole reporting stream on the subjects, but had concerns regarding the role of the CHIS in the criminality.

[redacted]

[redacted]

CHIS in Prisons [redacted]

13.19 The SHU managing CHIS in prisons comprises a Detective Inspector (who also manages the Source Targeting Unit), [redacted]. There is good liaison and co-operation with the Scottish Prison Service and a nominated senior manager from SPS provides concurrence on cases and also provides a single point of contact facility for Police Scotland.

13.20 I examined three CHIS cases of this particular category and have no concerns regarding how the cases are being managed by the Force. Authorising officers make clear at authorisation and renewal that should the CHIS be moved to another prison there should be a review conducted to address the risk to the CHIS, intelligence access in the new establishment, exit strategy etc.

13.21 The only points of note in relation to this particular category of CHIS are as follows:

[redacted]

[1] Association of Chief Police Officers in Scotland, Guidance on the Management of Covert Human Intelligence Sources (CHIS) Second Edition 2010

[redacted]

Counter Terrorism CHIS [redacted]

13.22 There has been a review during the past year and in recent months the source handling capability has been centralised into a single SHU comprising a [redacted] Previously there were [redacted] units, one in each geographical area of the Force, each comprising a [redacted]

13.23 The [redacted] and the benefits of having a [redacted] are already being felt with some cases being subjected to more robust governance and handlers being given clear and consistent instructions regarding the management of cases.

13.24 I examined several cases and found them to be well documented and being managed in a professional manner. Contact meetings were fully recorded and Risk Assessments were comprehensive and the newly agreed regime in this regard – following the recommendation of 2017 – was being carried out. Good use of the Policy Log facility was made by the controller and Authorising Officer. The previously reported delay in obtaining concurrence from the Security Service has been overcome.

13.25 The only adverse comment I have is in relation to one of the earlier authorisations granted by the newly appointed authorising officer [redacted] Whilst there was good consideration of the key issues of necessity, proportionality and collateral intrusion, there was a rather sweeping statement of the use and conduct along the lines that the CHIS was to report on 'matters relating to National Security'. Other authorisations granted more recently have had clearer parameters.

14 Undercover Operations [redacted]

14.1 Undercover operations authorised by Police Scotland continue to be managed by the Special Operations Unit (SOU) which is part of the Specialist Crime Division (SCD). The unit has strategic oversight and line management from a Detective Superintendent and Detective Chief Inspector who monitor the provision of resources and development of training and best practice but do not perform a role as defined under the legislation or Codes of Practice.

14.2 There are now in place [redacted] operationally and occupationally qualified Covert Operation Managers (COM-UCs) with [redacted] Detective Sergeants having attended and passed the relevant course delivered by the College of Policing. The COM-UC role will be split between the two distinct disciplines performed by the unit: the management of physical deployments and the management of deployments by officers in an 'on-line' capacity. The area of on-line undercover activity is growing and a long term operation currently being undertaken by the Force [redacted]) is subject to further comment later (at paragraph 14.8 of this report). Both officers performing the COM-UC role were interviewed and it is clear both officers have extensive experience in undercover policing and fully understand the need for clear lines of management to be in place to ensure that officers deployed (undercover officers and Cover Officers), understand the line management in place at any given time.

14.3 The establishment within the SOU was discussed at length during a visit to the undercover policing hub, at an offsite location. This discussion involved all staff on duty on the day of the visit and included officers trained as cover officers (CHIS handlers), those deployed as undercover officers (CHIS) in an online capability, and those trained to deploy physically as foundation or advanced officers. It was notable that there are currently [redacted] trained to deploy in an 'on-line' capacity. [redacted]

14.4 As alluded to, an inspection of a number of authorisations, reviews and the associated documentation for operations undertaken throughout the past year was undertaken. Applications to use undercover officers continue to be made by staff in the SOU before being passed to the COM-UC, accompanied by the associated risk assessments. The AO for the Force continues to be ACC Steve Johnson with the Chief Constable assuming the role once the operative reaches the renewal stage. ACC Johnson continues to support the SOU on a daily basis and continues with his intrusive and forward thinking approach as well as demonstrating 'grip' through his well formed authorisations and associated policy log entries. Additionally the Chief Constable shows similar 'grip' and intrusiveness. Both officers are supportive of this covert tactic and understand the value of it when dealing with serious crimes which affect the public of Scotland.

14.5 Overall the standard of associated documentation was high. A number of observations were made and conveyed to the COM-UCs which it is hoped will further strengthen the quality of the associated documentation. These observations relate to the inclusion, within the policy logs, of dates/times and details of discussions held with the Procurator Fiscal during the operational phases of undercover operations. By including these details within the relevant policy log a clearer picture emerges of discussions had and any potential legal issues which have emerged during the operational deployments. [redacted]

[redacted]

14.7 In the case of [redacted], discussions were held with the AO, ACC Johnson and the COM-UC, [redacted], regarding the necessity of the authorisation. The operational detail is not suitable to be discussed within this report, but related to the delivery of an illegally purchased item to specified and identified premises. [redacted]

14.8 Detailed discussions were held with the COM-UCs, cover officers and 'on-line' operatives for [redacted]

[redacted]

[redacted]

15 National Intelligence Assessment Unit [redacted]

15.1 The NIAU was created following a thematic inspection of intelligence processes and structures by Her Majesty's Inspectorate of Constabulary in Scotland. The intention is that this would enable a more joined up and holistic use of intelligence assets and have a Unit that would have access to the full range of intelligence assets and their product. Staff from the unit have a variety of specialist experience/training including financial investigations, internet investigations, CHIS handling, and analysis. The Unit sits within the Force Confidential Unit. [redacted]

16 Intelligence Development Unit [redacted]

16.1 The Intelligence Development Unit (IDU) has grown since the formation of Police Scotland and has benefited by having members from differing backgrounds and experience. In giving effective centralised support regarding high level criminality to the Specialist Crime Division, it is able, using small teams, to take on initial assessments and set up lifestyle surveillance. They work closely with the internal Internet Investigation Unit (IIU) which gathers wide ranging open source social media information which is pulled together to produce effective and time saving briefings. Further expertise is provided by the policy of having embedded officers originally from the NCA

but now also from HMRC who are able to add considerably to the effective consideration of more wide ranging cross border investigations. Over the last year three major operations were successfully pursued involving drug distribution; a second drug group who were also involved with adulterants; [redacted]. There is a helpful relationship with the CAB and Authorising Officers, and the proximity of other Units in the building was clearly of benefit to all.

17 CT Intelligence Unit [redacted]

17.1 This team undertakes similar work to the IIU (see paragraph 19.1) but in relation to counter terrorism matters and usually at the behest of, and in accordance with, directed surveillance authorisations provided by the Security Service. *R v Sutherland* is practised. Like the officers in the IIU, training and adherence to RIP(S)A was clearly evident from the helpful discussions.

17.2 [redacted]

17.3 Whilst there is internal oversight by the Detective Inspector of the work undertaken on line through open source or directed surveillance, the Unit would welcome external checks through the CAB or Force OpSy.

17.4 [redacted]

18 Financial Investigation Unit [redacted]

18.1 In addition to well proven techniques the Financial Investigation Unit (FIU) seeks to keep abreast of new approaches in order to identify the flow of illegal proceeds and to thwart where possible onward and more often instantaneous, distribution. Nevertheless, the universal problem of ever more sophisticated methods of disguise and dispersion is constantly challenging. Many of the inquiries are necessarily cross-border and international, and require considerable experience, application and co-operation. RIP(S)A powers have been successfully deployed [redacted] with a typical example being a case of the flow of illicit monies [redacted] The Unit has benefited from advice from the Authorising Officers and has a good relationship with the CAB.

19 Internet Investigation Unit [redacted]

19.1 This team undertakes open source research for other parts of the Force and will also manage any investigations for which a directed surveillance authorisation has been obtained in relation to social media. It comprises [redacted]

19.2 Jobs are allocated through the daily tasking meeting. [redacted] of its work relates to CSE cases, with referrals coming from CEOP. The officers are appropriately trained, and those who have an on line (Covert Internet Investigator) qualification tend to handle the directed surveillance cases as they appreciate where the line is drawn between monitoring and potential engagement with another person.

19.3 I discussed [redacted] and was reassured that the team does not slavishly begin work without considering the merits of the activity and whether it constitutes surveillance. I was also able to see the Access Database system the Detective Sgt manages, which records "live" jobs and colour codes key dates, such as expiry, reviews and so on. This is coupled with a simple but effective record of activity undertaken such as sites visited, when, for how long, and what screenshots have been captured, all numbered. [redacted], the IIU's recording systems struck me as a good example to adopt in preference to the somewhat paltry records seen elsewhere (paragraph 21.1).

20 Anti Corruption Unit [redacted]

20.1 We were provided with [redacted] involving ACU investigations by the relevant Authorising Officer. We inspected the paperwork for each (property interference, intrusive surveillance and directed surveillance used) but due to the sensitivities will not provide further details in this report. Suffice to say, we found the records in good order, although the intelligence cases were far too prolix (five sides of intelligence in one) and in one case, a little more could have been said with regards collateral intrusion involving young children which was unavoidable, but nonetheless worthy of mention at reviews over and above the basic activity log entry reference.

20.2 [redacted]

20.3 Any RIP(S)A or Police Act authorisations will be managed through the usual channels on Charter using the CAB for quality assurance and the main Authorising Officer cadre, unless there are particular sensitivities (although a ghost entry will be made on the Central Record to ensure all activity is captured). [redacted]

21 Divisional inspections [redacted]

21.1 [redacted] In relation to RIP(S)A compliance, discussions with the Head of Crime, Detective Superintendent [redacted] provided strong reassurance that the appropriate systems are in place. Professional discussions were held with a number of individuals and included applicants and intelligence managers. One key issue related to the use and management of Open Source Research. [redacted] It is appreciated that the organisation is considering the purchase and implementation of supportive software which will ensure a more compliant process.

22 Other Areas/Units visited

22.1 Covert Support Units [redacted]

The inspection visited a number of units across the organisation that support the delivery of Covert Policing including:

- The Covert Operations Unit
- The Specialist Support Unit
- The Technical Support Unit
- The Joint Operations Centre
- The Organised Crime and Counter Terrorism Unit [redacted]
- Covert Policing Support Unit

22.2 Each visit focused on systems and processes adopted across the organisation in relation to the deployment and management of surveillance and any associated equipment and no issues of note were found. Technical Support Unit staff raised the issue of training and felt that RIP(S)A awareness could be revisited across the unit; CAB staff who delivered training in 2016 have agreed to progress this at the earliest opportunity.

22.3 [redacted]

23 Good practice identified

23.1 The continuing overall good quality of RIP(S)A and Police Act documentation seen throughout the inspection. Achieved through the attention paid by the gatekeepers and the education, advice, guidance and training delivered by the CAB.

23.2 The continued commitment by the force to training provision and the CAB's efforts in this regard.

23.3 The commitment to his responsibility as Authorising Officer for "relevant sources" and the integrity of that process demonstrated by ACC Johnson.

23.4 The development of covert processes, including the development of the Covert Policing Support Unit and the processes developed by the OpSy, which have attracted recognition of good practice.

24 Conclusions

24.1 Final feedback was provided by [redacted] (relating to the communications data inspection) and [redacted] to the Chief Constable, DCC Gwynne, ACC Johnson and Detective Chief Superintendent Duncan Sloan. It was clear that the Chief Constable values the IPCO inspection and he seemed pleased to hear that his ethos of candid engagement, accompanied by a willingness to be the very best in terms of compliance, had been echoed throughout the week by all of his officers and staff.

24.2 The Force continues to impress with its high levels of compliance which is undoubtedly down to the efforts of the senior management team, departmental heads and their officers' eagerness to "get it right". This is a very positive report with the previous recommendations having been fully discharged and no further recommendations made during the 2018 inspection in relation to covert surveillance, property interference and CHIS. This is impressive, given the size of the Force and the wide range of covert operations undertaken throughout the year. This included the management of a particular covert operation, recognised as posing the highest of risks to law enforcement agencies and for which unique challenges were a daily occurrence.

24.3 That said, there are a number of significant matters highlighted regarding specific CHIS cases which have caused the inspection team some concern and which it is hoped the Force will review and take the appropriate action to address.

24.4 Additionally, whilst it is recognised that the Force has procured the [redacted] application for the gathering of empirical data to assist in the auditing of internet investigations, it is notable that there are currently disparate systems in place across the Force for auditing this activity. [redacted] Ordinarily the lack of a robust audit system would attract a recommendation, but given the overall compliance procedures in place across the Force and its recognition that the current auditing process is flawed, it is felt that time should be afforded to the Force to put new processes in place.

24.5 Our feedback sessions were well received and it is hoped that the matters highlighted to assist in further improving compliance, will be embraced and further strengthen what is a robust but supportive compliance regime.

24.6 As always, the inspection team were genuinely welcomed by everyone we encountered and were assisted throughout the week by the CAB team.

25 Recommendations

25.1 No recommendations are required as a result of this inspection in relation to the management of property interference, surveillance or CHIS.

[redacted]

[redacted]