Inspections under Chapter II of Part I of the Regulation of Investigatory Powers Act (RIPA) by the Interception of Communications Commissioner's Office (IOCCO)

Name of Public Authority	Leicester City Council
Date of Inspection	20th January 2011
Inspector	xxx

Background to the Inspection: The Interception of Communications Commissioner's Office (IOCCO) is charged with undertaking inspections on behalf of the Interception of Communications Commissioner, Sir Paul Kennedy. IOCCO undertake a revolving programme of inspection visits to all relevant public authorities who are authorised to acquire communications data under Part I Chapter II of the Regulation of Investigatory Powers Act (RIPA), and produce a written report of the findings for the Interception of Communications Commissioner.

The primary objectives of the inspection were to ensure that the system in place for acquiring communications data is sufficient for the purposes of the Act and that all relevant records have been kept; ensure that all acquisition of communications data has been carried out lawfully and in accordance with the Human Rights Act (HRA), Part I Chapter II of RIPA and its associated Code of Practice (CoP); and, provide independent oversight to the process and check that the data which has been acquired is necessary and proportionate to the conduct being authorised.

Statistics:

Number of applications which have been made during the previous 12 month period, and, if applicable, since the previous inspection.	**23 (36)**
Number of Authorisations granted under each section of the Act during the previous 12 month period, and, if applicable since the previous inspection.	**S21 4(a) - 0** **S21 4(b) - 0** **S21 4(c) - 41**
Number of Notices issued under each section of the Act during the previous 12 month period, and, if applicable since the previous inspection.	**S21 4(a) - 0** **S21 4(b) - 0** **S21 4(c) - 0**
Number of applications which have been rejected by a Designated Person during the previous 12 month period, and, if applicable since the previous inspection.	**Nil**

Staffing:

Senior Responsible Officer (SRO)	**xxx**
Accredited Officers (AOs)	**xxx**

Previous Recommendations:

The Council emerged well from the last inspection which took place in June 2009, and only two recommendations were made to improve the systems and processes. The first related to the giving of Section 22(4) Notices. Since the last inspection no Notices have been given as the Council has only acquired subscriber data and has been using Section 22(3) Authorisations to acquire this data. The second recommendation related to the SPoC making use of the streamlining procedure outlined in Paragraph 3.30 of the Code of Practice xxx. The Inspector is satisfied that the SPoC understands this procedure but was informed that it has not yet been necessary to use the procedure.

Summary of Inspection Findings:

Leicester City Council emerged well from the inspection. The Council is continuing to acquire communications data lawfully and for a correct statutory purpose. Importantly the Inspector found no evidence that the Council's powers under Part I Chapter II of RIPA had ever been used to investigate trivial offences.

Overall, the Inspector concluded that the applications were completed to a reasonable standard; however there is room for improvement, particularly in relation to the applications submitted by the City Wardens team. Some of these applications should not have passed the quality assurance checks which the Accredited Officer (AO) has a responsibility to conduct as they did not specify the statutory purpose for which the data was being acquired (i.e. Section 22(2)(b) prevention and detection of crime) which is a requirement of the Code of Practice. Furthermore there is also room to improve the proportionality justifications on the applications and some advice has been provided in this respect.

Overall the Single Point of Contact (SPoC) is still providing a good service to the Council, albeit there has been a little slippage in the quality of applications. It is recommended that AO should exercise his guardian and gatekeeper responsibility more robustly in future. There is also room to tighten the record keeping procedures.

The Inspector was satisfied that the Designated Person (DP) who had approved all of the applications in the last 12 months was discharging his statutory duties responsibly. The standard of his recorded considerations was generally good, but he should ensure that he always follows the good practice guidance by tailoring his comments to the individual applications.

The inspection findings are outlined in more detail in the following sections of the report. A number of recommendations arise from the inspection but they are designed simply to fine tune parts of the systems and processes and assist the public authority to achieve the best possible level of compliance with Part I Chapter II of RIPA and its associated Code of Practice. The recommendations are shown in the last column of the inspection tables. Please note that some of them are shaded red, amber or green. We have adopted this practice to enable public authorities to prioritise the areas where remedial action is necessary. The red areas are of immediate concern as they mainly involve serious breaches and / or non-compliance with the Act or Code of Practice which could leave

the public authority vulnerable to challenge. The amber areas represent non-compliance to a lesser extent. However remedial action must still be taken in these areas as they could potentially lead to breaches. The green areas represent good practice or areas where the efficiency and effectiveness of the process could be improved.

Summary of Recommendations: Red - 0; Amber - 3; Green - 3.

Areas Inspected:

1. Application Process

Acquisition of communications data under the Act involves four roles within a relevant public authority; the Applicant, the Designated Person (DP), the Single Point of Contact (SPoC) and the Senior Responsible Officer (SRO). The Act provides for two alternative means for acquiring communications data, by way of an Authorisation under Section 22(3) or a Notice under Section 22(4).

Baseline	Achieved (Yes / No / Partly)	Description of Procedures & Action Required (if applicable)	Rec No.
Examination of Applications			
A number of applications will be randomly examined by the Inspection team to check that the correct process has been applied and that the data has been obtained lawfully, with the approval of a Designated Person (DP). Public authorities must restrict the use of their powers under Part I Chapter II to obtaining communications data for investigations where they have a clear statutory duty and responsibility to conduct a criminal investigation and they should never be used to investigate trivial offences.	**Yes**	**Applications examined:** The 23 applications that had been submitted in the last 12 months were examined. The Inspector was satisfied the communications data had been acquired for the correct statutory purpose i.e. Section 22(2)(b) 'for the prevention and detection of crime.'	
Applicant			
The applicant should complete an application form, setting out for consideration by the designated person (DP), the necessity and proportionality of a specific requirement for acquiring communications data. (Para 3.3 CoP)	**Yes**	**Application / System used:** The applications are completed electronically and then printed off before being submitted to the AO. The hard copies are then delivered by hand to the DP together with any draft Section 22(4) Notices (if appropriate). The DP wet signs the applications together with any Section 22(4) Notices and returns them to the AO. **The Inspector advised that the Commissioner is happy to support the use of e-mail providing a clear audit trail exists and the e-mails and their attachments are retained centrally by the SPoC for this purpose. The application can be routed from the applicant to the AO and then onto the DP. The DP can then record his considerations and approval, insert the time and**	**1**

		date of issue on any Section 22(4) Notices and return the documents to the AO. It would then be appropriate to retain the records electronically and only print a hard copy when it is required. The SPoC log sheet could also be stored and updated electronically.	
Applications must include all of the requirements specified in Paragraphs 3.5 and 3.6 of the Code of Practice.	**Partly**	The Council are using the latest version of the Home Office and ACPO Data Communications Group (DCG) application form template and the majority included all of the requirements. However, a number of the applications that had been submitted by the City Wardens team did not specify the statutory purpose under Section 22(2). For some reason these applicants did not select Section 22(2)(b) 'prevent/detect crime' from the drop down menu. Instead the applicants typed 'RIPA' and in one case an applicant made a comment that all other options to obtain the required data had been exhausted which is of course totally irrelevant to the statutory purpose. **In future the statutory purpose under Section 22(2) must be included on every application form. The AO should provide a more robust guardian and gatekeeper role in this respect. The City Wardens team may require further training in relation to this point.**	**2**
Necessity: Applicants should outline a short explanation of the crime (or other purpose), the suspect, victim or witness and the phone or communications address and how all these three link together. A brief description of the investigation or operation may assist the DP to better understand the reason for the application. In a long term or complex investigation or operation it is important to set the application in context with the overall investigation or operation and set the scene and background. (See Home Office and ACPO DCG application guidance document).	**Yes**		
Proportionality: Applicants should outline what is expected to be achieved from obtaining the data and how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation. The specific date/time periods requested should be	**Partly**	It was not always clear from some of the applications what the applicant was trying to achieve by obtaining the data and this is a key part of the proportionality test. It should also be noted that where an applicant has requested the	**3**

justified i.e. how these are proportionate. An explanation as to how the data will be used, once acquired, and how this will benefit the investigation will assist the justification. (See Home Office and ACPO DCG application guidance document).		communications data for a particular date period, an explanation should always be given as to how this date period is proportionate to the offence/s under investigation. **It is recommended that in future all applicants should sufficiently justify the principle of proportionality by outlining what they are trying to achieve from obtaining the data and the relevance of any date / time periods requested. The AO should provide a more robust guardian and gatekeeper role in this respect and provide applicants with appropriate training / advice where this principle is not sufficiently justified.**	
Collateral Intrusion: Applicants should consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the privacy of any individual not under investigation may be infringed and why that intrusion is justified in the circumstance. Applicants should be aware that that there will only ever be minimal collateral intrusion in relation to subscriber data or that none will be identified at the time the application is made. (See Home Office and ACPO DCG application guidance document).	**Yes**		
Were any examples provided in relation to how communications data has been used to good effect (i.e. what use has been made by of the data acquired by the investigating officers? Did it lead to the identification of the offender? How was it of value to the investigation?)	**No**	The Council has made a limited number of applications for communications data and the data has been used to confirm or identify the subscribers of known telephones. There have not been any examples where the data acquired has been pivotal to the outcome of an investigation or trial.	
Single Point of Contact (SPoC)			
The SPoC should promote efficiency and good practice in ensuring only practical and lawful requirements for communications data are undertaken. (Para 3.16 CoP).	**Yes**		
The SPoC should provide objective judgement and advice to both the applicant and the DP. In this way the SPoC provides a "guardian and gatekeeper" function ensuring that public authorities act in an informed and lawful manner. (Para 3.16 CoP).	**Partly**	The Inspector saw examples where the SPoC had given advice to the DP. Applicants are also encouraged to speak to the SPoC prior to submitting applications. Some recommendations have already been made in this report to ensure the SPoC provides a more robust guardian and gatekeeper function in future relation to the quality of the applications.	

The SPoC should engage proactively with applicants to develop strategies to obtain communications data and use it effectively in support of operations or investigations. (Para 3.17 CoP).	**Yes**	Whilst none of the applications were in relation to complex investigations there is often dialogue between the applicant and SPoC prior to an application being submitted.	
The SPoC should be in a position to fulfil the additional responsibilities outlined in Para 3.17 CoP. There should be a full audit trail of all actions taken by the SPoC.	**Yes**	SPoC log sheets are completed and provide a good audit trail of the actions taken by the AO from the start to the end of the process.	
The SPoC may be an individual who is also a DP. The SPoC may be an individual who is also an applicant. The same person should never be an applicant, a DP and a SPoC. Equally the same person should never be both the applicant and the DP. (Para 3.19 CoP).	**Yes**	The AO has acted an applicant and a SPoC, but is not of the required rank to act as a DP.	
Designated Persons (DPs)			
A DP shall not grant an authorisation or give notice unless they believe that obtaining the data in question by the conduct authorised is proportionate to what is sought to be achieved by obtaining the data. (Section 22(5) Act). A DP must consider the application and record his considerations at the time (or as soon as is reasonably practicable) in writing or electronically. (Para 3.7 CoP). The DP shall assess the necessity for any conduct to acquire or obtain data taking account of any advice provided by the SPoC. (Para 3.10 CoP).	**Yes**	**No. of DPs:** 4. All of the applications examined had been approved by xxx, Director Environmental Services. However xxx the SRO; xxx, Head of Legal Services; and xxx, Strategic Director, Development, Culture & Regeneration can also act as DPs if required. The Inspector was satisfied that xxx was discharging his statutory duties responsibly and his considerations were generally completed to a good standard.	
IOCCO recommends that DPs should tailor their written considerations to the individual applications to provide evidence that they have been given due consideration.	**Partly**	In some of the applications the DP had followed the good practice guidelines by tailoring his considerations to the individual applications which is excellent. However, in others the DPs considerations were very short and generic phrases had been used. In such cases it would be more difficult for the DP to demonstrate that he had properly considered the justifications of necessity and proportionality if called upon to do so in Court or at a Tribunal. **It is recommended that the DPs should always follow the good practice guidance by tailoring their comments to the individual applications as this is the best means of demonstrating that they have been properly considered.**	**4**
DPs must ensure that they grant authorisations or give notices only for purposes and only in respect of types of communications data that a DP of their office, rank or position in the relevant public authority may grant or give. (Para	**Yes**		

3.9 CoP).			
DPs should not be responsible for granting authorisations or giving notices in relation to investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations or where it is necessary to act urgently or for security reasons. Where a DP is directly involved in the investigation or operation their involvement and their justification for undertaking the role of DP must be explicit in their recorded considerations. (Para 3.11 CoP)	**Yes**		
Content of Section 22(3) Authorisations and Section 22(4) Notices			
An authorisation must comply with all of the requirements outlined in Section 23(1) of the Act and Paragraphs 3.28, 3.43 & 3.44 of the Code of Practice.	**Yes**	The Home Office / DCG template is in use and was correctly completed. **The Inspector advised that there is no need to raise a separate Section 22(3) Authorisation or Section 22(4) Notice for each item of data requested if the telephone numbers or communications addresses are submitted on the same application and relate to the same CSP. Furthermore, the details of the Section 22(3) Authorisation are actually contained in Section 16 of the application form and this is where the DP grants the Authorisation. Therefore there is no need to send the Assurance of Authorisation document to the DP in the same way as a Section 22(4) Notice.**	***5***
A notice must comply with all of the requirements outlined in Section 23(2) of the Act and Paragraphs 3.37, 3.43 & 3.44 of the Code of Practice.	**N/A**	All the applications examined were in respect of subscriber information under Section 22(4)(c).	
The 'giving of a notice' means at the point at which a DP determines that a notice should be given to a CSP (Para 3.35 CoP). A notice should emanate from the DP and be endorsed in a clear and auditable manner.	**N/A**	Following a recommendation from the previous inspection, the SPoC is now fully aware that the Notices must emanate from a DP.	
SPoCs should be mindful when drafting authorisations and notices to ensure the description of the required data corresponds with the way in which the CSP processes, retains and retrieves its data for lawful. A notice must not place a CSP under a duty to do anything which is not reasonably practicable for the CSP to do. (Section 22(7) Act, Para's 3.29 & 3.38 CoP)	**Yes**		
Duration, Renewal & Cancellation of Section 22(3) Authorisations and Section 22(4) Notices			
Relevant to all authorisations and notices is the date upon which authorisation is	**Yes**		

granted or notice given. From that date, when the authorisation or notice becomes valid, it has a validity of a maximum of one month (see footnote 57 CoP). This means the conduct authorised should have been commenced or the notice served within that month. (Para 3.42 CoP).			
Any valid authorisation or notice may be renewed at any time before the end of the period of one month applying to that authorisation or notice, for a period of up to one month by the grant of a further authorisation or the giving of a further notice. A renewed authorisation or notice takes effect upon the expiry of the authorisation or notice it is renewing. (Sections 23(5), 23(6) & 23(7) Act, Para 3.46 CoP).	**N/A**	There have been no requirements to renew an authorisation or notice.	
Renewal may be appropriate where there is a continuing requirement to acquire or obtain data that will or may be generated in the future, The reasoning for seeking renewal should be set out in an addendum to the application. Where a DP is granting a further authorisation or giving a further notice they should have considered why it is necessary and proportionate to continue with the acquisition of the data and record the date, and when appropriate, the time of the renewal. (Para 3.47 & 3.48 CoP).	**N/A**		
Where a DP is satisfied that it is no longer necessary or proportionate to acquire the communications data he shall cancel the notice or withdraw the authorisation. (Section 23(8) Act, Para's 3.49, 3.50, 3.52 & 3.53 CoP). Reporting of a cancellation to a CSP may be undertaken on a DPs behalf by the SPoC, but in such cases the DP must confirm the decision in writing or in a manner that produces a record of the notice or authorisation having been cancelled or withdrawn by the DP.	**N/A**	There have been no instances when a cancellation of a notice or withdrawal of an authorisation has been appropriate.	
A cancellation notice must include the details outlined in Paragraph 3.51 of the Code of Practice. A withdrawal of an authorisation must include the details outlined in Paragraph 3.54 of the Code of Practice.	**N/A**		
National Priority Grading System (NPGS)			
Where relevant, the Data Communications Group (DCG) NPGS should be applied to requests for communications data correctly and fairly. (See Footnote 40 of the CoP). The emphasis within Grade 1 and Grade 2 is that the urgent provision of the specific	**Yes**	All requests for data by the Council have been correctly submitted as Grade 3.	

communications data will have an immediate and positive impact on the investigation.			
Streamlining Procedures			
The streamlining procedure outlined in Paragraph 3.30 of the Code of Practice should be used to reduce unnecessary bureaucracy and speed up the collection of the data when acquiring subscriber data under Section 21(4)(c). This procedure assists with number porting issues and enables the AOs to be more proactive when acquiring subscriber information by widening the data capture. In these instances it may be pertinent to acquire the data in stages. Furthermore, it is often good practice to check with the applicant before the data capture is widened because the direction of the investigation may have changed since the application was submitted or the user of the phone or communications address may have been identified through some other means.	**Yes**	The Council is now using Section 22(3) Authorisations to acquire all subscriber data which is good. The Inspector saw examples of this procedure being used when mobile telephone numbers had been ported to another CSP which has sped up the process. The Council has not found it necessary to use this procedure to widen the data capture xxx, but the AO understands the process and would use it if necessary.	
The streamlining procedure outlined in Paragraphs 3.31 and 3.32 of the Code of Practice which enable a DP to pre-authorise future subscriber checks at the same time as he or she is approving an application for service use or traffic data under Sections 21(4)(a) or (b) of RIPA, should be used to reduce unnecessary bureaucracy and speed up the collection of the data.	**N/A**	No applications have been made for service use data under Section 21(4)(b).	
The applicant must outline why it is necessary and proportionate to either widen the data capture under Section 21(4)(c), or obtain the consequential 'future' subscribers in their application. In the latter case they should outline what analytical work they intend to conduct on the service use / traffic data to identify the relevant numbers. It is important that the SPoC gives appropriate advice to the DP and that the DP fully understands what he or she is approving in the application form.	**N/A**	As mentioned above these procedures have not been used by the Council.	
The AOs should spot check the schedules to assure the integrity of the process, i.e. to check that the communications addresses derive from the original service use / traffic data requests and that secure open source checks have been conducted. This should provide a good safety net. Furthermore if an AO finds evidence that applicants or analysts are not following the correct procedures then this should be brought to the attention of the SRO.	**N/A**	As mentioned above these procedures have not been used by the Council.	

2. Training

It is important for all persons involved in the process to receive training and guidance to ensure that communications data is acquired lawfully in accordance with the Act and Code of Practice and used effectively in support of investigations.

Baseline	Achieved (Yes / No / Partly)	Description of Procedures & Action Required (if applicable)	Rec No.
The SPoC is either an accredited officer (AO) or group of AOs trained to facilitate lawful acquisition of communications data. All AOs must complete a course of training and have been issued a SPoC PIN number. (Para 3.15 CoP). When an AO leaves the SPoC their PIN number should be removed from the list of approved AOs.	**Yes**	**PIN list checked:** Yes	
DPs must have current working knowledge of human rights principles, specifically those of necessity and proportionality, and how they apply to the acquisition of communications data under Chapter II of Part I RIPA and its associated CoP. (Para 3.8 CoP).	**Yes**		
SPoCs should make efforts to ensure applicants are appropriately trained in the acquisition of communications data.	Partly	The SPoC has conducted training events for applicants from the Trading Standards, Environmental Crime and City Wardens teams and refresher training is given annually. The City Warden team have only recently begun to acquire communications data in support of their investigations but it is evident that most of the applicants do not fully appreciate the requirements when completing the application forms. Additional training may therefore be required and this forms part of two recommendations made earlier in the report.	

3. Keeping of Records

There are clear rules which must be followed in relation to the keeping of records and these procedures include the recording and reporting of errors. See Chapter 6 of the Code of Practice (CoP) for further information.

Baseline	Achieved (Yes / No / Partly)	Description of Procedures & Action Required (if applicable)	Rec No.
Records to be kept			
Applications, authorisations, copies of notices, and records of the withdrawal of authorisations and the cancellation of notices, must be retained by the public authority in written or electronic form, and physically attached or cross-referenced where they are associated with each other. The public authority should also keep a record of the date, and where appropriate the time, when each notice or authorisation is given or granted, renewed or cancelled. (Para 6.1 CoP).	**Partly**	See below detail.	
Records kept by the public authority must be held centrally by the SPoC or in accordance with arrangements previously agreed with the Commissioner. There records must be available for inspection by the Commissioner (Para's 6.1 & 6.2 CoP).	**No**	There is a duplication of effort in this area which is unnecessarily bureaucratic. When the application process has been completed, the SPoC retains copies of the documents. The original documents are retained in the Information Governance Department who oversee any processes relating to RIPA and maintain the central record (spreadsheet) of applications. However the Inspector found one example where the relevant documents were found in the SPoCs records, but not in the Information Governance records. **It is recommended that the SPoC assumes full responsibility for storing all original applications and associated documentation in order to comply with Paragraph 6.1 of the Code of Practice. These records can all be retained electronically (if they have been processed electronically). It is obviously a matter for the Council to decide if the Information Governance team also need to retain copies of these documents, but this does appear to be unnecessary and overly bureaucratic. It is also recommended that the SPoC assumes full responsibility for maintaining the central record (spreadsheet) and the AO agreed**	**6**

		to amend this to ensure that it also includes the type of data requested.	
Errors			
Where communications data is acquired or disclosed wrongly a report must be made to the Senior Responsible Officer (SRO) and then to the Commissioner ("reportable error") using the Error Reporting Form within no more than five working days of the error being discovered. (Para's 6.13 & 6.17 CoP). The error report must contain all of the details outlined in Para 6.18 of the CoP.	**Yes**	**No. errors 'reported' in previous 6 months:** One **Nature of errors (i.e. applicant, SPoC, CSP etc):** SPoC - One digit of a telephone number was incorrectly transposed onto the Section 22(3) Assurance of an Authorisation document and data was acquired in relation to the incorrect number.	
In cases where an error has occurred but is identified by the public authority or the CSP without data being acquired or disclosed wrongly, a record will be maintained by the public authority of such occurrences ("recordable error"). These records must be available for inspection by the Commissioner (Para 6.14 CoP). The records must include the details outlined in Para 6.20 of the CoP.	**N/A**	**No. errors 'recorded' in previous 6 months:** Nil **Nature of errors (i.e. applicant, SPoC, CSP etc):** N/A	
Where material is disclosed by a CSP in error which has no connection or relevance to any investigation or operation undertaken by the public authority receiving it, the material and any copy of it should be destroyed as soon as the report to the Commissioner has been made. (Para 6.21 CoP).	**N/A**		
Excess Data			
Where authorised conduct by a public authority results in the acquisition of excess data, or its disclosure by a CSP in order to comply with the requirement of a notice, all the data acquired or disclosed should be retained by the public authority. If having reviewed the excess data it is intended to make use of it in the course of the investigation an applicant must set out the reason(s) for needing to use that material in an addendum to the original application. The DP will then consider the reason(s) and consider whether it is necessary and proportionate for the excess data to be used in the investigation or operation. (Para's 6.23 to 6.25 CoP).	**N/A**	The Council has not acquired any excess data.	

National Anti-Fraud Network (NAFN) Single Point of Contact (SPoC)

During the inspection the Inspector discussed the SPoC facility which NAFN provides. NAFN has received funding from the Home Office so that it can act for any local authority which wishes to use its services and its AOs have been specially trained to the same standard as their police counterparts. NAFN uses an electronic system (Focus) to manage the applications and this system is used by a number of police forces and is fit for purpose. The NAFN AOs are also able to access a number of the online systems provided by the CSPs and therefore the data can be retrieved very quickly and with less expense.

In July 2010 NAFN were inspected by IOCCO and were found to have a very good level of compliance with the Act and Code of Practice. They are providing a good service to their local authority members who can use the NAFN SPoC facility with confidence and in the full knowledge that the data will be obtained in accordance with the law. The Home Office is encouraging all local authorities to use the facility. All of the records can be accessed and examined by the IOCCO inspectors from the NAFN offices. The Senior Responsible Officer (SRO) at NAFN is responsible for the integrity of the SPoC system and processes. However the Interception of Communications Commissioner believes that it is important for each local authority that uses NAFN to still appoint a Senior Responsible Officer (SRO) to oversee the process. If any issues arise from the inspection of the NAFN SPoC in relation to an individual local authority, the Inspectors will engage with that local authority's SRO to resolve them. The NAFN SPoC should inform the local authorities who are using their facility when an inspection is due to take place and should of course disseminate the findings.

As the Council is making relatively little use of its powers it may be more efficient and cost effective for the Council to use the NAFN SPoC. IOCCO would be grateful to receive notification of any decision concerning the use of the NAFN SPoC facility in order to facilitate future inspection planning and the collection of annual statistics on behalf of the Commissioner.

Freedom of Information Act (FOIA)

IOCCO is not a "public authority" for the purpose of the FOIA. It is therefore outside the reach of the Act, but it is appreciated that public authorities are not and that they may receive requests for disclosure of our reports. In the first instance the SRO should follow the procedure which is outlined in Paragraph 8.5 of the Code of Practice (Part I Chapter II of RIPA). No disclosure should take place until IOCCO have been fully consulted as it is very important that requests under the FOIA are dealt with in a consistent manner.

Conclusion & Requirement for Action:

IOCCO are extremely grateful for the excellent assistance and cooperation received during this inspection. The recommendations from this inspection are appended to the report in a schedule. It would be appreciated if you would ensure that the Senior Responsible Officer (SRO) oversees the implementation of the recommendations and ensures the schedule is completed and returned electronically to xxx by 25th March 2011. In light of the good level of compliance it will not be necessary to conduct a further inspection for at least 18 months.