ANGUS COUNCIL

POLICY AND RESOURCES COMMITTEE - 4 DECEMBER 2001 **ITEM No. 19**

REGULATION OF INVESTIGATORY POWERS (SCOTLAND) ACT 2000

REPORT BY DIRECTOR OF LAW AND ADMINISTRATION

ABSTRACT

This Report advises Committee of the requirements placed upon the Council by the Regulation of Investigatory Powers (Scotland) Act 2000 ("RIP(S)A"). This Report also makes recommendations with respect to the approval of a Council wide RIP(S)A policy and with regard to authorising covert surveillance under the Act.

1. RECOMMENDATIONS

The Committee is requested:-

(a) to note the duties placed upon the Council by RIP(S)A;

(b) to approve the RIP(S)A Policy attached as Appendix A; and

(c) to approve the appointment of "Authorising Officers" under the Act by the Chief Executive.

2. BACKGROUND

RIP(S)A is designed to regulate directed surveillance and the use of covert human intelligence sources by Public Authorities in Scotland. (Please see the Interpretation Section contained in Appendix A for a description of these and other terms under the Act.)

RIP(S)A came into force around the same time as the Human Rights Act 1998. This was no coincidence - without RIP(S)A giving a legal basis for covert surveillance, any covert surveillance undertaken by a public authority in Scotland would have breached Article 6 of the European Convention on Human Rights (ECHR) (the right to a fair trial); Article 8 of the ECHR (the right to respect for privacy) and, to a lesser extent, Article 1 of Protocol 1 of the ECHR (the right to respect for property).

"Directed Surveillance" is covert surveillance which is undertaken for the purpose of a specific investigation. ("Covert surveillance" is surveillance carried out in such a way to ensure that the person subjected to the surveillance is not aware of it.) This type of surveillance may require to be undertaken by various Council officers as part of their duties, for example:-

- Environmental Health Officers investigating the standards of cleanliness in a commercial restaurant;
- Housing Department officials investigating complaints of anti-social behaviour, such as noise emanating from neighbouring tenancies;
- Finance Department officials investigating fraudulent Housing Benefit or Council Tax Benefit claims;
- Trading Standards Officers covertly filming the activities of suspected dealers in counterfeit designer goods or computer software.

This list is not exhaustive and other Departments, such as Social Work, Planning, Personnel and Law and Administration may require to carry out covert surveillance from time to time.

In order for this type of surveillance to be lawful, it must be authorised and it must be carried out in accordance with that authorisation.

Failure to comply with the Act could have serious consequences. Evidence obtained during the investigation might prove to be inadmissible in Court (and lead to the Procurator Fiscal refusing to raise criminal proceedings referred to him by the Council). The Council could also be subject to a claim for damages in respect of a breach of the ECHR or be the subject of a complaint to the Tribunal established by the (English and Welsh) Regulation of Investigatory Powers Act 2000.

Although RIP(S)A came into force in October 2000, the codes of conduct prepared by the Scottish Executive on the Act have not been finalised and, in the interim, no covert surveillance falling within the definition contained in the Act has been undertaken by the Council. However, the Chief Executives of all local authorities in Scotland have been contacted by the Office of Surveillance Commissioners, advising that an inspection will be carried out of the procedures put in place by Scottish Local Authorities. As a result, although the Codes of Practice have not yet been finalised, it is appropriate to ask Committee to approve the Council's procedures under the Act. Committee should however note that the procedures may have to be amended once the Codes of Practice have been finalised.

3. PREPARATION FOR RIP(S)A

As mentioned in 2 above, in order for covert surveillance to be lawful, it must be authorised under the Act. Regulations made under RIP(S)A state that 'Heads of Service', 'Assistant Heads of Service' and 'Investigation Managers' - and any of their senior officers - may authorise covert surveillance. However, given the looseness of these terms, it is appropriate that certain officers be officially appointed as "Authorising Officers" in order to protect both the Council and the officers themselves from claims that surveillance has not been properly authorised under the Act. (Further information about the role of Authorising Officers is contained in the appended Policy and Guidelines. However, the main duties of Authorising Officers will be to consider whether surveillance should be authorised, authorise the covert surveillance and to review and where necessary renew the authorisation.)

Every Chief Officer has been contacted by the Chief Executive and has been asked to consider whether his or her Department requires to have one or more Authorising Officers appointed. A list of Authorising Officers has been prepared and, following the approval of this Report, the officers will be appointed by the Chief Executive to authorise surveillance under the Act. The Chief Executive will also require to amend the list of Authorising Officers from time to time in line with the needs of departments.

It is therefore recommended that Committee agrees to the proposed arrangements for the appointment of officers as Authorising Officers under the Act.

4. POLICY AND GUIDELINES

As already stated, appended to this Report is a Policy which also contains guidance on the Act. The Policy document summarises the requirements placed upon the Council by the Act, sets out procedures for granting authorisations (including suggested styles of application forms and register of authorisations) and lists the matters which must be considered prior to authorisations being granted. The document also sets out procedures for reviewing, renewing and cancelling authorisations and sets out how long information obtained as a result of investigations should be retained.

5. TRAINING

Awareness training on the Act and on the Policy and Guidelines has been arranged for all Council Officers who are to be appointed as "Authorising Officers". This training is to take place on 6 December 2001.

6. FINANCIAL IMPLICATIONS

Although RIP(S)A will impose new requirements on the Council, these will be mainly administrative and will be covered by existing budgets.

7. HUMAN RIGHTS IMPLICATIONS

There are no human rights implications arising as a direct result of this Report. However, as previously mentioned in this Report, RIP(S)A was introduced as a result of the ECHR, due to concerns about the possible breach of Articles 6 and 8 and Article 1 of Protocol 1. Provided that the requirements of RIP(S)A are complied with, then no breach of the ECHR should occur.

8. CONSULTATION

The Chief Executive and all Directors have been consulted in the preparation of this Report.

9. CONCLUSION

The Regulation of Investigatory Powers (Scotland) Act 2000 is an important piece of legislation, which regulates directed surveillance and the use of covert human intelligence sources by public authorities in Scotland. In order to safeguard the Council, it is important that the Council agrees policies and procedures for authorising covert surveillance under the Act.

CATHERINE A COULL
Director of Law and Administration

Note: No background papers, as defined by Section 50D of the Local Government (Scotland) Act 1973 (other than any containing confidential or exempt information), were relied on to any material extent in preparing the above Report.

ANGUS COUNCIL

POLICY AND GUIDELINES ON THE USE OF COVERT SURVEILLANCE

THE REGULATION OF INVESTIGATORY POWERS (SCOTLAND) ACT 2000 (DRAFT)

PART 1: POLICY BACKGROUND

1.1 INTRODUCTION

Angus Council is a public authority for the purposes of the Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A) and has the power to authorise directed covert surveillance and the use of covert human intelligence sources. Covert activities covered by RIP(S)A will be lawful if the activities are authorised and if they are conducted in accordance with the authorisation.

In some circumstances, it will be necessary for Council employees, in the course of their duties, to make observations of a person in a covert manner, ie, without that person's knowledge, or to instruct third parties to make such observations on the Council's behalf. By their very nature, actions of this sort are potentially intrusive (in the ordinary sense of the word) and may be legally challenged as breaching Article 6 (right to a fair trial), Article 8 (the right to respect for private and family life) and to a lesser extent Article 1 of Protocol 1 (the right to respect for property) of the European Convention on Human Rights (ECHR).

RIP(S)A provides, for the first time, a legal framework for the carrying out of covert surveillance by public authorities and an independent inspection regime to monitor these activities.

1.2 OBJECTIVE

The objective of this policy is to ensure that all covert surveillance carried out by or on behalf of Council departments is carried out effectively and lawfully. It should be read in conjunction with the Scottish Executive's Codes of Practice on Covert Surveillance ("the Codes of Practice").

If the procedures outlined in this policy are not followed, the evidence acquired as a result of the covert surveillance will have been acquired unlawfully. Such evidence may therefore not be admissible in Court, and the Procurator Fiscal is unlikely to take proceedings on the basis of such evidence. The Council may also be exposed to legal action for breaching the ECHR and may be the subject of a complaint to the tribunal set up by the (English and Welsh) Regulation of Investigatory Powers Act 2000.

1.3 SCOPE OF THE POLICY

This policy applies in all cases where "directed surveillance" or the use of a covert human intelligence source (CHIS) is being planned or carried out. Directed surveillance is defined in the Code of Practice as surveillance undertaken for the purposes of a specific investigation or operation which is likely to result in the obtaining of private information about a person. The policy does not apply to activities undertaken by the Council as a result of information discovered through the use of surveillance.

A CHIS is someone who establishes or maintains a relationship with another person with the intention of covertly obtaining information from that person.

The procedure does not apply to ad hoc covert observations that do not involve the systematic surveillance of specific persons. Equally, it does not apply to observations that are not carried out covertly or to unplanned observations made as an immediate response to events. However, in cases of doubt, the authorisation procedures described below should always be followed.

1.4 COVERT HUMAN INTELLIGENCE SOURCES

The use of a "covert human intelligence source" or "CHIS" (ie, council officers acting in an undercover capacity or the use of informants) raises similar issues to directed surveillance. The principles in this policy are equally applicable to such undercover operations, which must meet the same tests as directed surveillance and be properly authorised. However, additional rules apply to the use of a CHIS, and any service considering such activities should first consult the Department of Law and Administration on what is required. Council Officers making undisclosed site visits or test purchases do not count as "covert human intelligence sources" and such activities do not require formal authorisation.

PART 2: SEEKING AUTHORISATION

2.1 WHEN IS AUTHORISATION REQUIRED?

Authorisation is required for "directed surveillance", ie, surveillance which is covert but not intrusive. This means surveillance for the purposes of a specific investigation or operation, whether or not the identity of those who will be observed by the surveillance is known in advance.

The surveillance must be undertaken in a manner which is likely to acquire private information about one or more people ('private information' is not defined, but includes information about a person's private and family life). The surveillance must also be conducted in such a manner as is calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place. As a result, the use of overt CCTV systems (where the cameras are plainly visible and signs advising of the presence of the cameras are displayed) does not require authorisation under the Act, but placing a hidden camera to discover who is, eg, stealing from a vending machine does. The surveillance must take place otherwise than by way of an immediate response to events, the nature of which is that it would be impractical to seek authorisation before carrying out the surveillance. (See 2.2 below). Authorisation is required whether the activity is carried out by Council Officers themselves or by third parties carrying out surveillance on behalf of and under the instructions of the Council (such as private investigators or the neighbours of anti-social tenants).

2.2 All covert activities which come within the scope of RIP(S)A must have written authority, except in an immediate response to circumstances that amount to covert conduct. The officer must decide whether the surveillance is necessary and proportionate and note it as such. Such activities should not exceed one day. In any case, authorisation should be sought at the first possible opportunity. Where it is impossible to obtain written authorisation, oral authorisations may be sought. Where this happens, the Investigation Manager must complete an application form on behalf of the requesting officer as fully as possible in order to justify the oral authorisation. Oral authorisation should not exceed 72 hours and full written authorisation should be obtained at the first possible opportunity.

2.3 WHO MAY SEEK AUTHORISATION?

Any officer whose duties involve a surveillance activity falling within the description of directed surveillance contained in 2.1 may seek authorisation to do so and must seek and be granted authorisation (subject to the circumstances narrated in 2.2 above) prior to carrying out the surveillance. This is most likely to arise in departments responsible for regulatory, enforcement or security functions. Standard application forms for directed surveillance authorisation and for covert human intelligence sources are attached to this policy.

2.4 INTRUSIVE SURVEILLANCE

Intrusive surveillance means surveillance in relation to anything taking place in any private vehicle or on any residential premises, ie, a person's accommodation (even if only temporarily used), but not surveillance on common areas such as common stairs and closes. The Council is not authorised to conduct intrusive surveillance under any circumstances.

Some additional points should be made about intrusive surveillance. Firstly, surveillance is not intrusive if it is directed into a home or private vehicle from outside of that home or vehicle unless the information provided from the surveillance is consistently of the same quality as would be provided by having a device actually present in the home or vehicle. Advice from the Office of the Surveillance Commissioners (OSC) suggests that the sort of surveillance undertaken by local authorities is unlikely to reach this level of sophistication. As a result, activities such as filming goods being sold from the back of a car or monitoring the level of noise generated by an antisocial tenant (but not the actual words spoken by the tenant) are unlikely to be classed as intrusive, and so these activities can be safely carried out, subject of course to appropriate authorisation.

Secondly, devices carried into a home or private vehicle by a covert human intelligence source do not constitute intrusive surveillance provided that the CHIS has been invited in. However, the device must not be left behind when the CHIS leaves the premises or vehicle. Departments are reminded of the need to have proper authorisation (and the need to satisfy other requirements) before any use is made of a CHIS.

2.5 WHEN IS COVERT SURVEILLANCE APPROPRIATE?

By its very nature, covert surveillance intrudes on people's privacy. It should therefore be regarded as a final option, only to be considered when all other methods have either been tried and failed, or where the nature of the activity the surveillance relates to is such that it is reasonable to conclude that covert surveillance is the only way to acquire the information being sought. Using the earlier example, if a vending machine is regularly broken into, consideration should be given to installing overt CCTV cameras (with appropriate signage in terms of the Data Protection Act 1998) rather than installing hidden cameras.

2.6 PROPORTIONALITY

Proportionality is a concept of Human Rights Law designed to ensure that measures taken by the state (and organs of the state such as the Council) which impact on the rights of citizens are kept within proper bounds. It means that if the same legitimate end can be reached by less intrusive means, then the less intrusive path should be taken. There should also be a reasonable relationship between the seriousness of the mischief being addressed and the degree of intrusion into people's lives.

Covert surveillance involves a potentially serious breach of individuals' rights to privacy under Article 8 of the ECHR. Compelling reasons are therefore required to justify using covert surveillance, particularly if the surveillance is to continue for an extended period. Surveillance of a staff member on sick leave is likely to be disproportionate if all that is being assessed is a possibly fraudulent claim for a very small amount of statutory sick pay, but it may be proportionate in detecting a fraudulent legal claim against the Council for thousands of pounds.

In deciding whether any planned surveillance is proportionate, it is useful to consider how serious the breach you are seeking to rectify is. For criminal offences, the potential punishment by the Court (eg level of fine or length of prison sentence) may be a useful guide. However, many regulatory offences attract only very small fines, but are designed to prevent potentially life threatening situations (such as the sale of dangerous goods or contaminated food, or the overcrowding of licensed premises). Such factors weigh in favour of surveillance being proportionate.

2.7 CONFIDENTIAL MATERIAL AND COLLATERAL INTRUSION

Confidential material covers a number of areas: professional legal advice given to someone, health information, spiritual counselling and material held under an obligation of confidentiality (particularly for the purposes of journalism). So far as possible, surveillance operations should be designed so as to minimise or eliminate the possibility of confidential information being acquired. If confidential information is in fact acquired, special care should be taken to avoid unnecessary disclosure of it. (Reference should be made to the Council's Data Protection Act Policy.)

"Collateral Intrusion" refers to the fact that often surveillance operations will inadvertently intrude on the privacy of persons other than those at whom the operation is directed. Operations should be planned so as to minimise or eliminate so far as possible the risk of collateral intrusion. When it is likely that the surveillance will intrude on other people's privacy, this will be a factor to consider in determining the proportionality of the operation.

2.8 SURVEILLANCE BY OTHER PUBLIC AUTHORITIES

Council Officers are occasionally asked to assist in surveillance operations being conducted by other public authorities such as the Police, the Benefits Agency, Customs & Excise etc. In such cases it is for the organisation seeking assistance from the Council to ensure that it has appropriate authorisations in place. These authorisations should be shown to the Council staff involved or else staff should receive written confirmation from the other authority that the authorisations have been duly granted. If the Council is carrying out its own surveillance as part of a joint operation, however, it will be necessary for the Council to put its own authorisations in place too.

PART 3: GRANTING AND RECORDING AUTHORISATIONS AND REFUSAL

3.1 WHO MAY GRANT AUTHORISATIONS?

In terms of Regulations made under RIP(S)A, authorisations for direct surveillance may only be granted by the "Head of Service", "Assistant Head of Service", an "Authorising Officer" or their senior officers. The Chief Executive has designated the holders of a number of officers in Angus Council as Authorising Officers. The Line Managers of any designated Authorising Officers may also grant authorisations.

Departments without a designated Authorising Officer should seek authorisation from the Chief Executive. However, where departments find - perhaps because of a change in their duties - that they will regularly require authorisation, they should request the Chief Executive to appoint an Authorising Officer specifically for their department.

In general, an Authorising Officer should be a third tier officer or above. The officer authorising surveillance must not be operationally involved in the surveillance being authorised. As a result, departments should ensure that a sufficient number of members of staff have been appointed as Authorising Officers.

3.2 RECEIPT AND LOGGING OF APPLICATIONS

All Departments carrying out surveillance activities must maintain a record of applications made for directed surveillance, together with a record of the consent or refusal. A suggested style of register of authorisations is attached to this document. This register, together with all of the forms used for applying for authorisation or renewing or cancelling authorisation must be retained safely. The register and forms may be monitored for cross-department consistency by the Director of Law and Administration and will have to be produced in the event of an inspection by the OSC. These forms represent evidence of the Council's compliance with RIP(S)A and the Codes of Practice and, as such, care should be taken in the completion and logging of them. Departments must ensure that the forms are easily retrievable and held in a central location in each department as it is likely that only two weeks' notice will be given before the OSC carry out an investigation.

3.3 GRANT OR REFUSAL OF AUTHORISATIONS

The OSC may require an authorising officer to justify his/her decision to grant a request, so authorisation should never be granted automatically. Evidence of reasoned refusal of requests is also vital in displaying compliance with the law.

The Authorising Officer's job is to be satisfied that the officer seeking approval:-

- has correctly identified a lawful purpose for the proposed surveillance;
- has planned the operation properly so as to minimise collateral intrusion and the collection of confidential information;
- is not proposing to stray beyond the permissible bounds of directed surveillance; and
- has correctly applied the proportionality test.

Only if actively satisfied about all of these points should the authorisation be granted. Any restrictions imposed on the authorisation should be noted on the authorisation form.

3.4 DURATION, RENEWAL AND CANCELLATION OF AUTHORISATIONS

By law, an authorisation lasts for three months. However, for Council purposes, it is suggested that authorisations generally should only be granted for one week. Surveillance which has failed to uncover evidence within one week is a questionable use of resources, quite apart from the fact that long-term surveillance is harder to justify in terms of proportionality. If the justification for carrying out the surveillance ceases to apply, the authorisation should be cancelled and a record kept of the cancellation and the reasons for the cancellation. (Where an authorisation period comes to an end, a cancellation form need not be completed.)

If the surveillance is to be continued for longer than the original period, a renewal must be authorised. Renewal applications must highlight the fact that what is sought is a renewal and should have attached the original authorisation and any previous renewals. The tests applicable to renewals are identical to those for initial applications. Again, forms for renewals are attached.

In the case of authorisations granted for more than one week, there should be a weekly review by the Authorising Officer. This review should note whether any significant evidence has been acquired by the surveillance and whether, against that background, continued surveillance can still be justified. Weekly reviews should be noted on the authorisation form.

3.5 SECURITY AND RETENTION OF DOCUMENTS

Documents created under this procedure are highly confidential and must be treated as such. Departments must make proper arrangements for their retention, security and destruction, in accordance with the requirements of the Code of Practice and the Data Protection Act 1998. Refusals, as well as approved applications, must be retained. The Code of Practice recommends retaining the authorisations for five years (longer if required for ongoing proceedings).

In accordance with guidance issued by the OSC, documents will be inspected periodically by the Director of Law and Administration to ensure that a consistent approach is being adopted by different Council Departments. The OSC also has statutory powers of inspection and all records (applications, authorisations and refusals) must be available for inspection. No record should be destroyed until after an OSC Inspector has had the opportunity to see them.

Each Department carrying out surveillance activities must make appropriate arrangements for the secure storage of authorisations and refusals. The Director of Law and Administration must be advised of these arrangements.

APPENDIX ONE - INTERPRETATION

PART A - GLOSSARY OF TERMS

(a) Covert surveillance

Surveillance is covert if, and only if, it is carried out in a manner calculated to ensure that the subject of the surveillance is unaware that it is taking place (see 1(8)(a) of RIP(S)A).

(b) Directed surveillance

Surveillance is directed if it is covert but not intrusive and is undertaken for the purpose of a specific investigation in such a manner as is likely to result in obtaining private information about a person and is otherwise than by way of an immediate response to events, the nature of which is such that it would not be reasonably practicable for an authorisation to be sought (see 1(2) of RIP(S)A).

(c) Covert human intelligence source

A "CHIS" is a person who establishes or maintains a relationship with another in order to obtain information covertly (see 1(7) of RIP(S)A).

(d) Intrusive surveillance

Intrusive surveillance is covert surveillance carried out in relation to anything taking place on any residential premises or in any private vehicle, which involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device which consistently provides information of the same quality and detail as could be obtained from a device naturally present in the residential premises or vehicle (see 1(3) and (5) of RIP(S)A).

(e) Private information

This includes any information relating to a person's private or family life (see 1(9) of RIP(S)A).

PART B - PRINCIPLES OF SURVEILLANCE

(a) Lawful Purposes

Covert surveillance can only be carried out where it is necessary to achieve one or more of the permitted purposes (as defined in RIP(S)A). Covert surveillance must therefore be

- for the purpose of preventing or detecting crime or the prevention of disorder; or
- in the interests of public safety; or
- for the purpose of protecting public health.

Employees carrying out surveillance must not cause damage to any property or harass any person.

(b) Necessity

Covert surveillance shall only be undertaken where there is no reasonable and effective alternative way of achieving the desired objective(s).

(c) Effectiveness

Planned covert surveillance shall be undertaken only by, or under the supervision of, suitably trained or experienced employees.

(d) Proportionality

The use and extent of covert surveillance shall not be excessive, ie, all covert surveillance must be in proportion to the significance of the matter being investigated. If there is a way of obtaining the information in a less intrusive manner, then that less intrusive manner should be used.

(e) Intrusive Surveillance

No activities shall be undertaken that come within the definition of "intrusive surveillance", ie, if the activity involves surveillance of anything taking place in residential premises or in a private vehicle. (However, see 2.4 below.)

(f) Collateral Intrusion

Reasonable steps shall be taken to minimise the acquisition of any information which is not directly necessary for or relevant to the purposes of the investigation being carried out.

(g) Authorisation

All directed surveillance must be authorised in accordance with the procedures described below.