Section V

# The Role of External Review Bodies

Chapter 21

# Resolving Citizens' Grievances

Security and intelligence agencies are often trusted with exceptional powers, such as surveillance or security clearance, which, if used incorrectly or mistakenly, carry the risk of serious injustice to individuals. It is therefore important that some avenue of redress should be open to people who suspect that they may have been the victim of an injustice, for example those whose private life may have been intruded upon or whose career may have been affected. Moreover, in a security or intelligence agency, as with any large body, complaints can highlight administrative failings and lessons to be learned, leading to improved performance. However, precisely because of the secret nature of the processes involved, difficulties in obtaining evidence, and the legitimate need of these agencies to protect sensitive information from public disclosure, redress through public hearings in the regular courts is rarely effective or appropriate. There is also the need to ensure that any system for redress cannot be used by the legitimate targets of a security or intelligence agency to find out about the agency's work. Achieving a balance in any complaints system between independence, robustness and fairness, on the one hand, and sensitivity to security needs on the other is challenging but not impossible.

The essential distinction in these different systems is between:

- Non-judicial processes (ombudsmen or parliamentary committee);
- Judicial-type procedures (courts and tribunals).

## Non-Judicial Handling of Complaints

Different oversight systems handle complaints in a variety of ways. An independent official, such as an ombudsman, may have power to investigate and report on a complaint against an agency (this is the case in the Netherlands, see Box No. 51 overleaf). In some countries an independent Inspector-General of security and intelligence deals with complaints against the services as part of the office's overall oversight remit in a rather similar way (see Chapter 21). This is the case in New Zealand and South Africa for example. In addition, specific offices established under freedom of information or data protection legislation may have a role in investigating complaints against the agencies.

Ombudsman-type systems place reliance on an independent official investigating on behalf of the complainant. They usually exist to deal with an administrative failure rather than a legal error as such. They give less emphasis to the complainant's own participation in the process and to transparency. They typically conclude with a report, and (if the complaint is upheld) a recommendation for putting matters right and future action, rather than a judgement and formal remedies.

Box No. 51:
Handling of Complaints: the Dutch National Ombudsman

Article 83
Each person is entitled to file a complaint with the National Ombudsman on the actions or the alleged actions of the relevant Ministers, the heads of the services, the coordinator and the persons working for the services and for the coordinator, with respect to a natural person or legal entity in the implementation of this act or the Security Investigations Act.

Source: Intelligence and Security Services Act 2002, The Netherlands, Art. 83.

Complaints and grievances of citizens can also be dealt with by the parliamentary intelligence oversight committee, as is the case in, for example, Germany and Norway (see Box No. 52 below).

Box No 52:
Handling of Complaints: the Norwegian Parliamentary Intelligence Oversight Committee

'On receipt of complaints, the Committee shall make such investigations of the administration as are appropriate in relation to the complaint. The Committee shall decide whether the complaint gives sufficient grounds for further action before making a statement.

Statements to complainants should be as complete as possible without revealing classified information. Statements in response to complaints against the Security Service concerning surveillance activities shall, however, only declare whether or not the complaint contained valid grounds for criticism. If the Committee holds the view that a complainant should be given a more detailed explanation, it shall propose this to the Ministry concerned.

If a complaint contains valid grounds for criticism or other comments, a reasoned statement shall be addressed to the head of the service concerned or to the Ministry concerned. Statements concerning complaints shall also otherwise always be sent to the head of the service against which the complaint is made.'

Source: Instructions for monitoring of intelligence, surveillance and security services (EOS), Section 8, pursuant Section 1 of the 1995 Act on Monitoring of Intelligence, Surveillance and Security Services, Norway.

Although handling complaints is separate from parliamentary oversight, there is a connection. Parliamentarians are often called on to represent the grievances of individual citizens against government departments. There may be a benefit also for a parliamentary oversight body in handling complaints brought against security and intelligence agencies since this will give an insight into potential failures – of policy, legality and efficiency. On the other hand, if the oversight body is too closely identified with the agencies it oversees or operates within the ring of secrecy, there may also be disadvantages in it handling complaints. The complainant may feel that the

complaints process is insufficiently independent. In cases where a single body handles complaints and oversight it is best if there are quite distinct legal procedures for these different roles. On the whole it is preferable that the two functions be given to different bodies but that processes are in place so that the oversight body is made aware of the broader implications of individual complaints.

In some countries not only citizens but also members of the services are permitted to bring service-related issues to the attention of an ombudsman or parliamentary oversight body. For example, in Germany officials may raise these matters with the Parliamentary Control Panel 'although not when acting in their own interest or in the interest of other members of these authorities, insofar as the head of the service has failed to look into matters in question. Members of staff may not be cautioned or penalised for doing so.'[1]

## Judicial Handling of Complaints

Alternatively, a specialist tribunal may be established to deal with complaints either against a particular agency or in relation to the use of specific powers, as in the United Kingdom. Or complaints may be handled by a specialist oversight body, as in Canada (see example in Box No. 53 below).

Box No. 53:

### Handling of Complaints: the Canadian Security Intelligence Review Committee

Under the Canadian Security Intelligence Service Act 1984 the Security Intelligence Review Committee ('SIRC'), the statutory oversight body composed of Privy Counsellors, is also responsible for investigating complaints brought by individuals 'with respect to any act or thing done by the Service' (section 41) as well as challenges brought to denials of security clearance (section 42). Complainants using these provisions must first raise the matter with the government department concerned and must complain to SIRC in writing. Investigations take place in private, although the complainant is given an opportunity to make representations (s. 46) and to be represented by counsel. Neither the complainant nor the Service is entitled to see the representations of the other. SIRC possesses powers of subpoena and to hear evidence on oath (s. 50). Concerning the report of findings, the Review committee shall:

(a) on completion of an investigation in relation to a complaint under section 41, provide the Minister and the Director with a report containing the findings of the investigation and any recommendations that the Committee considers appropriate; and

(b) at the same time as or after a report is provided pursuant to paragraph (a), report the findings of the investigation to the complainant and may, if it thinks fit, report to the complainant any recommendations referred to in that paragraph.

Source: Canadian Security Intelligence Service Act, 1984.

Judicial procedure does not always involve court hearings. A tribunal has some advantages over a regular court in dealing with security – and intelligence-related complaints: it can develop a distinct expertise in the field of security and intelligence,

judges and lawyers can be vetted as necessary, and specific procedures can be devised for handling sensitive information. In view of the nature of the subject matter these are unlikely to involve a full public legal hearing. On the other hand, while some tribunals may give the complainant a hearing, he or she is likely to face severe practical difficulties in proving a case, in obtaining access to relevant evidence, or in challenging the agency's version of events. To combat some of these problems special security-cleared counsel have been introduced in Canada and in the UK. These counsel have the task of challenging security-related arguments, especially those aspects not disclosed to the complainant. This can help the tribunal reach a more objective assessment of the evidence and the arguments.

## The ECHR and the Handling of Complaints

For states which are signatory to the ECHR there are considerations about the requirements of different Convention rights under Articles 6, 8 and 13 which need to be observed in designing complaints mechanisms. Article 6 gives the right to a fair trial by an independent and impartial tribunal in criminal matters and in the determination of a person's civil rights and obligations. Article 6 has been taken to apply, for example, to procedures governing evidence from informants and undercover state officials in a criminal trial,[2] and to rules restricting the treatment and disclosure of evidence in the public interest, both in criminal and civil trials.[3] The use of special security-cleared counsel has been commended by the European Court of Human Rights as a way of meeting the requirements of the right to a fair trial Article 6 of the ECHR.[4]

However, even where Article 6 does not apply, procedural protections may be required in complaints processes, because of Articles 8 and 13. These articles impose some *ex post facto* controls in the case of security measures which intrude upon privacy, such as surveillance and security vetting. There is, however, no European Convention blueprint (for example, a person subject to surveillance need not always be informed after the event).[5] Article 13 recognises the right to an effective remedy before a national authority for violation of a Convention right. This need not be a court in every case and in security-related issues the European Court of Human Rights has found that a combination of different oversight and complaints mechanisms may be adequate.[6] As a Council of Europe Working Party put it:

> On the basis of the Court's case-law on Articles 8 and 13 of the Convention it can be concluded that whether the requirement of an effective remedy is satisfied, does not depend only on the mere existence of access to a court, but on the entire arsenal of oversight mechanisms and their effectiveness.[7]

The key criteria of a credible complaints system are that it should:

- Be clearly independent of the security or intelligence agency,
- Have the necessary powers and access to information in the hands of the agency for resolving the complaint
- Be able to award effective remedies in the event of upholding a complaint, and an adequate explanation of the reasons for refusing a complaint.

It is useful if some form of assistance is available to complainants unfamiliar with legal process to help them in lodging a complaint. It should also give an opportunity for the complainant to participate sufficiently in the investigation or proceedings so that the process is seen to be fair, whether or not a formal hearing is given. The process of investigation may need to restrict the information or reasons made available to a complainant for reasons of national security. However, this should be to the minimum extent necessary, it should always be the decision of the person or body handling the complaint, rather than of the agency under investigation, and should be compensated for by other procedural protections (for example, the use of Special Counsel to challenge the agency's case).

## Best Practice

- ✓ The official or tribunal hearing the complaint should be persons who fulfil the constitutional and legal requirements to hold an office at this level and should enjoy legal security of tenure during their term of office;
- ✓ As much of the process as possible should be completed in public. Even where the process is closed to the public as much of it as possible should be open to the complainant and his or her legal representatives;
- ✓ There should be a power to dismiss without investigation complaints that the official or tribunal concludes are vexatious or frivolous;
- ✓ If it is necessary for reasons of national security to restrict the participation of a complainant in the review process then the decision to do should be in the hands of the reviewing official or tribunal alone and compensating safeguards (such as the use of a 'Devil's Advocate' or 'Special Counsel') should be provided to ensure that proceeding are fair and impartial;
- ✓ The tribunal or official should have power to make legally binding orders which provide an effective remedy to a complainant who has a justifiable case. These may include the award of compensation and the destruction of material held by the security or intelligence agencies;
- ✓ The scope of review and grounds of review should be clearly established in law and should extend to the substance (rather than merely procedural aspects) of the actions of the security or intelligence agencies.

Chapter 22

# Oversight of Agencies within the Administration by Independent Authorities

If, to avoid the dangers of political manipulation, security agencies are given some constitutional 'insulation' from political instructions, how can the government be assured that it has all the relevant information and that secret agencies are acting according to its policies?

For this reason a number of countries have devised offices such as Inspectors-General, judicial commissioners or auditors to check on the activities of the security sector and with statutory powers of access to information and staff.[8]

The idea was first devised in the US intelligence community, which now has around a dozen inspectors-general. All are independent of the agencies concerned. There are, however, significant variations: some of these offices are established by legislation (for example, the Inspectors-General for the Central Intelligence Agency and the Department of Defense), others rest solely on the administrative arrangements established by the relevant Secretary (for example, with regard to the Defense Intelligence Agency and the National Reconnaissance Office). Irrespective of this distinction some report to Congress as well as to the executive branch. A number of these offices have a remit that extends to efficiency, avoiding waste and audit, as well monitoring legality and policy compliance.

Inspectors-General of this kind are within the ring of secrecy: their function is not primarily to provide public assurance about accountability, rather it is to strengthen accountability to the executive. Canadian legislation contains a clear illustration of this type of office.

The Canadian Inspector-General has unrestricted access to information in the hands of the Service in order to fulfil these functions.

Box No. 54:
The Functions of the Canadian Inspector-General

The Inspector-General is responsible to the official in charge of the relevant government department (the Deputy Solicitor-General) and has the role of

(a) monitoring the compliance by the Service with its operational policies;
(b) reviewing the operational activities of the Service; and
(c) submitting an annual certificate to the Minister stating the extent to which the Inspector General is satisfied with the annual report of the Service and whether any of the Service's actions have contravened the Act or ministerial instructions or have involved an unreasonable or unnecessary exercise by the Service of any of its powers.[9]

Source: Canadian Security and Intelligence Service Act, 1984, Sections 30 and 32.

Similarly, in Bosnia and Herzegovina the Inspector-General is responsible under Article 33 of the Law on the Intelligence and Security Agency for providing 'an internal control function'. To this end, the Inspector-General may review the Agency's activities, investigate complaints, initiate inspections, audits and investigations on his or her own initiative, and issue recommendations. The Inspector-General has a duty of reporting at least every six months to the Security Intelligence Committee and of keeping the main executive actors informed of developments in a regular and timely fashion. The powers of the Inspector-General include questioning agency employees and obtaining access to agency premises and data.

Other countries – notably South Africa[10] – have created Inspectors-General to report to Parliament. In these cases the office in effect bridges the ring of secrecy ie it is an attempt to assure the public through a report to Parliament that an independent person with access to the relevant material has examined the activities of the security or intelligence agency. However, inevitably most of the material on which an assessment of the agency's work is made has to remain within the ring of secrecy, although it may be shared with other oversight bodies.

Even some inspectors-general whose statutory brief is to report to the executive may maintain an informal working relationship with parliamentary bodies, this is so in Australia for instance and, as noted above, a number of the US inspectors-general report periodically to Congress.

Whether an office of this kind reports to the government or to Parliament, in either case, careful legal delineation of its jurisdiction, independence and powers are vital. Independent officials may be asked to review an agency's performance against one or more of several standards: efficiency, compliance with government policies or targets, propriety or legality. In any instance, however, the office will need unrestricted access to files and personnel in order to be able to come to a reliable assessment. In practice an independent official is unlikely to be able to scrutinise more than a fraction of the work of an agency. Some of these offices work by 'sampling' the work and files of the agencies overseen – this gives an incentive for the agency to establish more widespread procedures and produces a ripple effect. Some also have jurisdiction to deal with individual complaints (as under the Australian scheme).[11]

## Best Practice

- ✓ Review of the functions of the security and intelligence agencies affecting individuals should be by independent and impartial officials (such as Ombudsmen, or Inspectors-General) and comply with the following standards;
- ✓ The official who acts as a reviewer should be a person who fulfils the constitutional and legal requirements to hold an office at this level and should enjoy legal security of tenure during their term of office;[12]
- ✓ The scope of review and grounds of review should be clearly established in law and should extend to the substance (rather than merely procedural aspects) of the actions of the security or intelligence agencies;
- ✓ The official should have sufficient legal powers to be able to review matters of fact and evidence relating to the use of powers of the security or intelligence agencies;
- ✓ The official should have ultimate authority to determine the form and scope of any order or report or decision which results from the process.

Chapter 23

# Independent Audit Offices

The executive's and parliament's financial oversight responsibility is far from finished once the intelligence service's budget has been adopted. Not only the executive, but also parliament has to enforce its oversight and audit functions, keeping in mind that the presentation of fully audited accounts to parliament is part of the democratic process and that the auditing process should entail both the auditing of accounts and the auditing of performance. The accounts and annual reports of the security and intelligence services are an important source of information for parliaments to assess how public money was spent in the previous budget year.

## Guaranteeing Independence

In most countries the national audit office, (sometimes called the Auditor-General, National Audit Office, Budget Office or Chamber of Account) is established by constitutional law as an institution independent of the executive, legislative and judicial branches. In order to guarantee its independence, the Auditor-General:

- ✓ Is appointed by parliament and has a clear term of office;
- ✓ Has the legal and practical means and resources to perform his/her mission independently;
- ✓ Has the independent authority to report to parliament and its budget committee on any matter of expenditure at any time.

Parliament should see to it that judicial sanctions are provided for by law and are applied in cases of corruption and mismanagement of state resources by officials and the political body. Parliament should also see to it that remedies are applied in case of fault.

## Auditing Security and Intelligence Services

The objective of audit of the security and intelligence services is to certify that the expenditure is in compliance with law in an effective and efficient manner. To this extent, it is essential that the services are open to full scrutiny by the Auditor-General apart from limited restrictions to protect the identities of certain sources of information and the details of particularly sensitive operations.[13]

Precisely because the services function under the protection of secrecy, shielded from public scrutiny by the media and civil society watchdogs, it is important that the auditors have wide access to classified information. Only in this way, it can be certified whether the services have used public funds within the law or whether illegal practices, eg corruption, have occurred.

Box No. 55:
### The Auditor General

"Regardless of whether it falls under the Executive, the Legislature or the Judiciary, it is imperative for the Audit Office to be completely independent and truly autonomous. It should also dispose of adequate resources to accomplish its mission. Its function is three-fold:

#### Financial Oversight
The Audit Office must verify the accuracy, reliability and thoroughness of the finances of all organs of the Executive and public departments. It must verify that all financial operations are carried out in accordance with the regulations on public funds. Within the context of this oversight function, the Audit Office must fulfil a mission of jurisdiction with regard to public accountants and officials who authorise payments. They must all be made accountable for the money they handle save in the case of a discharge or release of responsibility. In cases of misappropriation or corruption, the Audit Office is duty-bound to report its findings to the Judiciary.

#### Legal Oversight
The Audit Office must verify that all public expenditure and income are conducted in accordance with the law governing the budget.

#### Ensuring Proper Use of Public Funds
A modern Audit Office which functions in the interest of good governance should ensure the proper use of public funds on the basis of the three following criteria :

(i) *Value for money*: ensure that the resources used were put to optimal use, both qualitatively and quantitatively;
(ii) *Effective*: measures to what extent objectives and aims were met;
(iii) *Efficient*: measures whether the resources used were used optimally to obtain the results obtained.

This *ex-post* oversight is conducted on the initiative of the Audit Office or at the request of Parliament.

*Excerpts from: General Report on the IPU Seminar on Parliament and the Budgetary Process, (Bamako, Mali, November 2001)*

As a matter of a general principle of good governance, the normal rules of auditing which apply to other activities of government, should also apply to the audit of the expenditures of the services with some limited restrictions as mentioned above. What makes auditing security and intelligence services different from regular audits, are the reporting mechanisms. In order to protect the continuity of operations, methods and sources of the services in many countries special reporting mechanisms are in place. For example, in the UK, as far as the parliament is concerned, only the Chairman of the Public Accounts Committee and the Intelligence and Security Committee are fully briefed about the outcome of the financial audit. These briefings may include reports on the legality and efficiency of expenditures, occurrence of possible irregularities, and whether the services have operated within or have exceeded the budget. In the case of Germany, the control of the accounts and the financial management of the intelligence services is carried out by a special institution (i.e. *Dreierkollegium*) within the national audit office (*Bundesrechnungshof*). The *Bundesrechnungshof* reports its

secret findings on the control of the accounts and the financial management of the intelligence services to a special sub-committee of the Parliamentary Budget Control Committee (i.e. the Confidential Forum), the Parliamentary Control Panel for intelligence oversight, the Federal Chancellery (*Bundeskanzlerarmt*) as well as to the Finance Ministry.[14] The parliament (i.e. not the intelligence services) decides which elements of the intelligence services' budget need to be secret.[15]
Furthermore, in many countries, the public annual reports of the security and intelligence service (eg in the Netherlands) or of the parliamentary oversight body (eg in the UK) include statements about the outcome of the financial audits.[16]

The box below illustrates how the disclosure of information about the services to the auditor can be arranged.

Box No. 56:
Statutory Disclosure of Information of the Services to the Auditor (UK)

'[T]he disclosure of information shall be regarded as necessary for the proper discharge of the Intelligence Service if it consists of (…) the disclosure, subject to and in accordance with arrangements approved by the Secretary of State, of information to the Comptroller and Auditor General for the purposes of his functions.'

Source: Intelligence Services Act 1994, Section 2(3)b, United Kingdom

It also happens in many countries that the audit office investigates the legality, effectiveness and efficiency of particular projects, such as the building of a new headquarters (eg in Canada and the UK) or the purchase of new SIGINT (Signal Intelligence) systems (eg in the UK) or the exchange of information between the services for coordinating anti-terrorism policy (the Netherlands). Box No. 58 gives an example of the mandate and scope of an investigation by the Canadian Auditor-General.

The national audit office does not function in a vacuum, but is embedded in an existing system of financial accountability procedures, provided for by law. Normally, laws on financial accountability in general and laws on intelligence services in particular, specify which normal and special accountability provisions apply. Box No. 57 gives an example of some of the financial accountability procedures of the Luxembourg intelligence services. The Luxembourg illustrates three significant elements of financial auditing systems. Firstly, the special accountant of the intelligence services is appointed by the relevant minister, and not by the director of the intelligence service. This provision puts the accountant in a strong position within the service and contributes to the independence of his office. Secondly, the mandate of the national audit office is to check periodically the way in which the services are managed from a financial point of view. This implies that the mandate goes beyond accessing and accounting for the legality of the expenditure and also includes consideration being given to the performance, efficiency and efficacy of the services in question.

Thirdly, the law stipulates that the Law on State Budget, Accountability and Treasury also applies to the intelligence services (except for some specific exemptions). Therefore, the objective of the law is to reach a situation where the normal practices of good financial management are applied as much as possible.

Box No. 57:
### Financial Accountability (Luxembourg)

'(1) The expenditures of the Intelligence Services are carried out by the special accountant of the Intelligence Service, who is appointed by the minister in charge of the budget in accordance with the provisions of article 68 of the amended 8 June 1999 Law on State Budget, Accountability and Treasury.
(2) Exceptions to the provisions of article 68 - 73 of the aforementioned law are:
- The periodical control of the management of the Intelligence Service is done by the National Audit Office;
- The funds that are received by the special accountant are allocated to the payment of the expenditures of the Intelligence Service; and are recorded in the accounts of the special accountant;
- At the end of each trimester, the special accountant reports on the use of the funds to the official who has the power to authorise expenditures, within the timeframe that is indicated in the decision to allocate the funds;
- The funds which are not used for paying the expenditures during the fiscal year for which they are allocated, are not returned to the State Treasury. Instead, these funds are recorded in the Intelligence Service's attributes for the following fiscal year;
- The official who has the power to authorise expenditures, submits the special accountants' financial records to the National Audit Office for its approval;
- The National Audit Office submits the accounts, together with its observations to the Prime Minister, Minister of State;
- At the end of each fiscal year, the Prime Minister, Minister of State, offers the minister to whom the responsibility for the budget has been attributed, the option of discharging the special accountant from his functions. The discharge should be decided upon before 31 December of the fiscal year following the fiscal year to which the accounts of the special accountant refer to.'

Source: Loi du 15 juin portant organisation du Service de Renseignement de l'Etat, Article 7, Memorial - Journal Officiel du Grand-Duché de Luxembourg, A-No. 113 (unofficial translation)

Box No. 58:

### Independent Audit of Projects: the Example of the National Headquarters Building Project of the Canadian Security and Intelligence Services (CSIS) by the Auditor General of Canada

'Objectives: The objectives of the audit were to determine whether the constructed national headquarters facility would meet the CSIS-stated objectives and the Treasury Board approvals, and whether the project was implemented with due regard to economy and efficiency.

Criteria: Our audit criteria were derived from our guide for auditing capital asset projects, as well as the appropriate Treasury Board policies and guidelines.

Scope: The audit examined all the major stages of this major Crown project. Specifically, we reviewed the needs definition, the options analysis, the project definition, the design and review process, the contracting process, change orders, project management, environmental assessment, commissioning and post-project evaluation. Our audit commenced in November 1995 and was completed in March 1996. Given the size and complexity of this project and the limited time available, we did not audit detailed financial records. (…) The audit did not address the CSIS mandate. However, in acquiring an understanding of the requirements for the facility, we confirmed that they were based on the existing mandate and were appropriate.

Approach: Audit evidence was collected through extensive interviews with the building project staff, and with CSIS staff as users of the building. We reviewed planning documents, submissions to the Treasury Board, project briefs, minutes of the Senior Project Advisory Committee meetings and project management meetings, correspondence, contract documents and annual reports. We inspected the building, from the roof to the basement, including the office space, special purpose space and building services space. We received a high level of cooperation (…). The level of cooperation is particularly noteworthy given the security considerations relative to CSIS operations and the facility itself.'

Source: 1996 Report of the Auditor General of Canada, available at http://www.oag-bvg.gc.ca

A cautionary note, however, is important. Security and intelligence services are not entirely comparable to other the business of government. For a number of reasons, the work involves a higher degree of risk, and, therefore, investments may go wrong due to factors outside the responsibility of the service. Elected representatives should treat the outcomes of the audits with great care. An unbalanced response to the reports of the auditor general or the leaking of its results could hurt the operations, harm the services' functioning, and, last but not least, might damage the trust between the political leadership and the leadership of the services.

## Best Practice

- ✓ In order to guarantee the independence of the audit office, its operation should be based on law, it should report to parliament and the director of the audit office should be appointed or confirmed by parliament;
- ✓ The law on audit offices should include provisions on the office's mandate, reporting mechanisms, the appointment of the director as well as on access to classified information;
- ✓ The auditor-general should have full access to classified information, with specific restrictions in order to protect the identity of sources and sensitive operations;
- ✓ The statutory audit offices should be able to conduct not only financial audits but also performance audits of specific projects in detail;
- ✓ As the audit offices are dealing with classified information, safeguards should be put in place to avoid unauthorised publication of (parts of) audits.

## Endnotes Section V - The Role of External Review Bodies

1. German *Bundestag* Secretariat of the Parliamentary Control Commission (PKGR), *Parliamentary Control of the Intelligence Services in Germany,*(Berlin: *Bundespresseamt*, 2001), pp. 19-20.
2. *Windisch v Austria*, (1991) 13 European Human Rights Reports 291; *Van Mechelen v Netherlands*, (1998) 25 European Human Rights Reports 647, *Teixeira de Castro v Portugal*, European Court of Human Rights, Judgment of 9 June 1998.
3. *Rowe and Davis v UK*, (2000), 30 European Human Rights Reports 1; *Tinnelly and McElduff v UK*, E Ct HR, Judgment, 10 July 1998.
4. *Chahal v UK,* (1997) 23 E.H.R.R. 413; *Tinnelly and McElduff* v *UK*, (1999) 27 E.H.R.R. 249.; *Edwards and Lewis v UK*, European Court of Human Rights, Judgment 22 July 2003 and 27 October 2004.
5. *Klass v Germany*, para. 15 (as regards Art. 8); *Leander v Sweden*, para. 68 (as regards Art. 13).
6. *Leander v Sweden, para. 78.*
7. 'Report on the Feasibility of Recommendations on Internal Security Services', adopted by the *PC-S-SEC* at its second meeting (9 - 11 October 2002), p. 15.
8. For comparison of the powers of Inspectors-General in different countries, see: Intelligence and Security Committee (UK), *Annual Report for 2001-2*, Cm 5542, Appendix 3.
9. CSIS Act, s. 33.2. Both the Service's Annual Report and the Inspector-General's certificate are required to be sent to the oversight body, SIRC.: s. 33.3 CSIS Act 1984.
10. Office of the Inspector General of Intelligence.
11. Inspector-General of Security and Intelligence Act 1986, sections 10-12.
12. See, for example, Law of the Intelligence and Security Agency of Bosnia Herzegovina, Article 32:
    'An Inspector General shall be appointed and dismissed by the Council of Ministers upon the proposal of the Chair. The Inspector General shall serve a four-year term, which may be renewed once. The Inspector General may be dismissed before the expiration of his/her mandate upon his/her own request; if s/he permanently loses the capacity to execute his/her duties; fails to comply with applicable legislation or regulations; fails to implement measures for supervision of the Agency; if criminal proceedings for the criminal offences of abuse of office or disclosing a State, military or official secret have been instituted against him/her; if a final imprisonment sentence for a criminal offence which makes him/her unworthy of executing such duties is rendered against him/her; or if s/he fails to conduct an investigation, inspection or audit in a timely and lawful manner.'
13. These restrictions apply to the UK Comptroller and Auditor-General, see Report by the Comptroller and Auditor-General, *Thames House and Vauxhall Cross,* HC Session 1999-2000, 18 February 2000, point 8. Available at:
    http://www.nao.org.uk/publications/nao_reports/9900236.pdf
14. German *Bundeshaushaltsordnung* (BHO) (1969), Para. 10a (3); Secretariat of the German Parliamentary Control Panel, *Die Parlamentarische Kontrolle der Nachrichtendienste in Deutschland – Materialien*, (Berlin: Bundestag, 2003), p. 42; Website of the German Intelligence Service (*Bundesnachrichtendienst*) at:>http://www.bundesnachrichtendienst.de/auftrag/kontrolle.htmBundeshaushaltsordnung>.
15. German Bundeshaushaltsordnung (BHO) (1969), Para. 10a (2).
16. See, for example, Annual Report of the General Security and Intelligence Services of the Netherlands (2003), available at:
    <http://www.minbzk.nl/contents/pages/9459/annual_report_2003_aivd.pdf>, pp. 69-70; Intelligence and Security Committee Annual Report 2002-2003, presented to parliament by the Prime Minister by Command of Her Majesty, June 2003, London, pp. 8-13.