Commission of Inquiry
into the Actions of Canadian Officials in Relation to Maher Arar

Policy Review

Accountability and Transparency

A Background Paper
to the Commission's
Consultation Paper

December 10, 2004

In a democratic society, *accountability* is a key value. Accountability means having an obligation to answer for, or explain, one's actions. Elected officials are expected to be held accountable to the voters for their record in office. Governments are accountable for the expenditure of taxpayers' dollars. Appointed officials are expected to be accountable for their conduct of public administration. Even private corporations and associations, such as churches and trade unions, are increasingly expected to be accountable for their actions taken in trust, as it were, on behalf of the society.

Accountability takes a number of specific forms. Generally, we can address a number of questions to help specify more precisely what forms of accountability are being looked at:

- accountability *for what?*
- accountability *to whom?*
- accountability *by whom?*
- accountability *of whom?*
- accountability *when?*

In addition, the accountability relationship is understood in two very different senses, sometimes as *controlling*, and sometimes as *explanatory*.[1] When accountability implies control, it means that those held accountable are *subordinate* and *obedient* to those to whom they account – for instance, public servants accountable to the responsible minister. When accountability implies explanation, it means that those held accountable *cooperate* with those to whom they account – for instance, an agency providing information on its activities to an independent review body. In practice, accountability often implies both control and explanation, but to different authorities. Accountability within an organization to a minister or executive generally means control, but the same organization may also be accountable to an authority that does not exercise direct control over its activities, but can require cooperation in providing information about those activities. For example, a department of government exercises internal management of

[1] Geoffrey Marshall, 'Police accountability revisited', in D. Butler and A. Halsey, eds., *Policy and Politics* (London: Macmillan, 1978), pp. 51-65.

the financial operations of its sections, but the same department is also subject to the external scrutiny of the Auditor General and the Public Accounts Committee of the House of Commons. Both are examples of accountability, but internal management represents accountability as control, while the external audit represents accountability as explanation.

Accountability sometimes takes on yet another face. Mechanisms of accountability seem to imply a relationship of power or influence over those held to account, whether these are exercised through control or through cooperation. But accountability may also offer *legitimacy* to those persons or organizations held accountable. By effectively managing the presentation of information about their activities, organizations can communicate a favourable image of themselves.[2] In this sense, external review bodies are sometimes said to have been 'captured' by those agencies they are charged with reviewing. This is not an inevitable, but a possible outcome, of the working of accountability. Those designing accountability mechanisms must be aware of this potential.

Examining accountability from the perspective of improving government performance, former senior public servant and student of public administration David A. Good cites three ways of looking at accountability from the inside, as it were:[3]

- Accountability for control
- Accountability for assurance
- Accountability for learning

Accountability for control means controlling the abuse and misuse of public authority. Accountability for assurance, on the other hand, is concerned about providing assurance

---

[2] Richard Ericson identifies *'account ability'* to describe "the capacity to provide a record of activities that explains them in a credible manner so that they appear to satisfy the rights and obligations of accountability." Richard V. Ericson, 'The news media and account ability in criminal justice', in Philip C. Stenning, ed., *Accountability for Criminal Justice: Selected Essays* (Toronto: University of Toronto Press, 1995) p. 137.

[3] David A. Good, *The Politics of Public Management: the HRDC Audit of Grants and Contributions* (Toronto: University of Toronto Press, 2003), pp. 166-73, citing Peter Aucoin and Ralph Heintzman, 'The dialectics of accountability for performance in public management reform', *International Review of Administrative Sciences* 66:1 (March 2000) pp. 43-53.

to Parliament and citizens that public authority and tax dollars have been used appropriately and ethically. Accountability for learning means ways by which the assessment of performance becomes the stimulus for promoting improvement. Good cautions that each of these forms of accountability hides tensions and contradictions, especially when all three are pursued simultaneously by organizations. He concludes that "any single accountability perspective is partial, incomplete, and in competition with the others. It is by skilfully combining and balancing all three that we are likely to see the most progress."[4]

Secrecy and accountability

Accountability and transparency go hand in hand. Yet public administration is never fully public. Much of the business of government necessarily takes place behind closed doors, just as much of the business of private corporations is kept securely out of the public eye and away from the scrutiny of competitors. In both cases, there are good reasons for secrecy. Sometimes, of course, there are bad reasons invoked for secrecy, and it is the job of audit and review bodies to expose these bad reasons and determine if something is being covered up that requires publicity. But by the same token, accountability must recognize and respect the legitimate grounds for secrecy, and work within the limitations on transparency that these impose.

As the sociologist of bureaucratic organization, Max Weber, pointed out long ago, it is characteristic of bureaucracy that its operations are as secretive as possible.[5] A leading observer of British government terms administrative secrecy "Whitehall's cardinal virtue and dominant characteristic" and suggests that "secrecy is the bonding material which holds the rambling structure of central government together….Of all the rules of government, secrecy is the most sacred."[6] The Canadian political scientist Donald Savoie

[4] Good, *op. cit.*, p. 179.
[5] H.A. Gerth and C. Wright Mills, eds., *From Max Weber: Essays in Sociology* (London: Routledge, 1970) pp. 233-4.
[6] Peter Hennessy, *Whitehall* (London: Fontana Press, 1990) pp. 345-6.

comments that “things are not much different in Canada...Secrecy and confidentiality have also permeated government operations in Canada.”[7]

One of the reasons for secrecy is the highly competitive and partisan nature of Parliament. Information about government is used by the opposition as a source for criticism. Governments try to minimise political risk by reducing transparency, and managing the presentation of information in ways that enhance their political credibility. Government and opposition are only fulfilling their respective roles in a competitive democratic environment, but the result is that secrecy is the rule, while disclosure is the exception, either forced or managed, as the case may be. It has always been an operating principle of the Westminster system of government that cabinet deliberations remain strictly confidential; “cabinet confidences” (including not only cabinet minutes and decisions, but cabinet documents) are excluded from the *Access to Information Act*.

Of course, there are also legal and ethical reasons for maintaining forms of administrative secrecy. The larger government has become, the more its operations penetrate and influence the society, the greater the need to maintain secrecy about its plans, lest private interests gain financial or competitive advantage from ‘inside information’. Thus the requirement for secrecy surrounding the preparation of budgets with their tax implications, or the requirement of secrecy around preparing regulatory instruments for the private sector.

Secrecy in government may be inevitable, but the acceptable degrees and limits of secrecy are often issues of controversy. This is especially the case where accountability is in question. The administrative requirements of confidentiality and the need for relative transparency in holding governments accountable are in persistent tension with one another. Accountability fails when secrecy is excessive, or is deliberately and illegitimately employed for covering up incompetence or wrongdoing. Yet an accountability mechanism that fails to respect the legitimate reasons for secrecy will be

[7] Donald J. Savoie, *Breaking the Bargain: Public Servants, Ministers, and Parliament* (Toronto: University of Toronto Press, 2003) p. 44.

unacceptable and unworkable. Accountability mechanisms are designed to negotiate the sometimes complex path between secrecy and transparency. Striking an appropriate balance is key to successful accountability architecture. This is easier said than done, of course.

Accountability in national security

If accountability and secrecy are generally in tension, this is all the more so in matters of national security and law enforcement. These present particular problems, not usually encountered in other areas of government. Security, intelligence and policing agencies have special and necessary requirements for secrecy that exceed the requirements for secrecy in other areas of government operations.

In the past, and even today in some countries, the proposition that the activities of intelligence and policing agencies must be kept strictly secret even to the extent of denying the desirability of any form of external review or oversight, has been taken as almost self-evident. Threats to national security that are clandestine and designed to elude detection can only be met with equivalent secrecy and concealment on the part of those charged with assessing and countering these threats. As an unchallenged general proposition, this argument would seem to rule out any effective external accountability mechanism for such agencies, leaving oversight and control as exclusively internal, either by the agencies themselves or by their political masters, but with no transparency. This argument is no longer accepted in Canada, where forms of external review have been implemented for security intelligence and policing agencies over the past few decades. If the *general* requirement for secrecy can no longer be taken to exclude external review, it is nonetheless the case that the *specific* requirements for secrecy must be taken fully into account in designing any accountability mechanisms in this area. We can look at these specific requirements in turn.

Secrecy of sources

Security and intelligence agencies have always relied upon *human sources* of intelligence. They have always been adamant that the identities of their sources, and the

identities of agents operating under cover, must be protected to the fullest extent possible. The anonymity of sources is key to their recruitment and retention: whatever the motive for cooperating (which may range from idealism to coercion to financial incentives, or mixtures thereof), potential human sources must be assured that their double identities will not be revealed. The moment the identity of a source is disclosed, the usefulness of that source is terminated. In many cases, as with the penetration of violent organizations, the protection of the identity of a source may be literally a matter of life or death.

The *CSIS Act* makes it a criminal offence punishable by up to five years imprisonment for unauthorized disclosure by an official or former official of the identity of "a confidential source of information or assistance" to CSIS or "any person who is or was an employee engaged in covert operational activities of the Service."[8] The *Access to Information Act* contains exemptions for information that "would reveal the identity of a confidential source of information" in criminal law enforcement investigations, or "any record requested under this Act that contains information the disclosure of which could reasonably be expected to threaten the safety of individuals."[9] The disclosure of confidential sources has sometimes been an issue when deciding whether to initiate criminal prosecution in national security cases that rest on the testimony of confidential sources. Part 3 of the *Anti-terrorism Act* contains a number of amendments to the *Canada Evidence Act*[10] seeking to protect against the disclosure in open court of the identities of sources in anti-terrorist cases[11].

Secrecy of investigative methods and tradecraft

Equally important to intelligence and law enforcement agencies is the protection of information about their methods of investigation, including technical means of intrusive surveillance. Since the targets of security surveillance and criminal investigations constitute covert or concealed threats to the security of Canada, the methods used to identify and assess these threats, and, on occasion, to prosecute, must necessarily be

[8] *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23 (*CSIS Act*), s. 18(1).
[9] *Access to Information Act*, R.S.C. 1985, c. A-1, s. 16(1)(c)(ii) and s. 17. Similar exemptions can be found in the *Privacy Act*, R.S.C. 1985, c. P-21, s. 22(1)(b)(ii) and s. 25.
[10] R.S.C. 1985, c. C-5.
[11] S.C. 2001, c. 41, Part 3, ss. 43-46.

protected from disclosure, as any such information could assist those targeted to evade detection. Investigative methods may encompass a wide range of matters, from targeting to budgeting of resources, from operational technology to the 'tradecraft' of the agency's operatives (the accumulated experience and culture of how they go about their business). As with the case of human sources, investigative methods are protected against disclosure under the *Access to Information* and *Privacy* acts, and may also be blocked from disclosure in court under the strengthened evidence provisions of the *Anti-terrorism Act.*

Secrecy of information received in confidence from abroad

A major reason for secrecy, especially in recent years, is the use by Canadian intelligence and law enforcement agencies of information received in confidence from foreign governments and their agencies, or from international organizations. A large proportion of the intelligence on which Canada relies to assess threats to Canadian security results from intelligence exchanges and information sharing with co-operating agencies in friendly countries. Much of the intelligence that Canada receives is designated as confidential and released only on the guarantee that it will not be publicly revealed. In some cases, the intelligence may even be designated only for the specific agency with which it is shared; the latter being expected to restrict circulation even with its sister agencies. Canada, in turn, shares its intelligence with co-operating foreign agencies on the same basis of confidentiality. Breaches of these arrangements could result in a breakdown of the networks of intelligence exchange, which could seriously damage the effectiveness of security and law enforcement co-operation in Canada and abroad. Thus Canadian agencies are insistent that confidentiality regarding all information received from allied and co-operating agencies must be protected from unauthorized disclosure. There are a number of legal guarantees in place here as well, embedded in various Canadian statutes, including the new *Security of Information Act*, and in evidentiary procedures in Canadian courts when disclosure could be considered injurious to the conduct of international relations.

These three areas of secrecy – identity of human sources; investigative subjects and methods; and relationships with other police and security intelligence services in Canada

and abroad including information received in confidence from such agencies – together broadly define the matters that most concern security and law enforcement agencies with regard to the security of information. If the need for secrecy is evident, the precise boundaries defining what must remain secret, and what may be disclosed, are not always clear and are often the basis for controversy. When it comes to accountability, the agencies may have legitimate concerns about secrecy that are even greater than those of normal government bodies. It is, however, no longer accepted that they should be able to act, in effect, as sole judges in their own cases in defining what must remain secret and what may be disclosed. Disclosure decisions are normally subject to judicial review, even if it is necessary to hold *ex parte* proceedings, where secret material is reviewed *in camera.* Accountability mechanisms for national security typically operate with some mixture of publicity and secrecy. Review bodies have access to information that cannot be disclosed, or even in some cases explicitly referenced in public, but this need not deter them from reporting their findings publicly, with as much indication concerning confidential material as can be reasonably summarised. Occasionally, disputes over disclosure between agencies and those bodies reviewing their activities may require adjudication. But in no case should the requirements of secrecy any longer be taken as a complete bar to external accountability.

Secrecy, moreover, is not merely a matter of insiders vs. outsiders. Within the executive branch of government, security and intelligence agencies have privileged access to secrecy not generally available to other departments and agencies. To the extent that they can withhold information from other parts of the executive, they are less accountable. Even within security and intelligence agencies, there are well-known practices of *compartmentalization* and the '*need to know'* principle that limit the transparency of operations to colleagues, let alone outsiders. This is a problem that only accentuates the need for accountability within government as well as from the outside. [12]

[12] The late US Senator, Daniel Moynihan, from his extensive experience in oversight of US intelligence, stressed that: "Departments and agencies hoard information, and the government becomes a kind of market. Secrets become organizational assets, never to be shared save in exchange for another organization's assets….[T]he system costs can be enormous. In the void created by absent or withheld information, decisions are either made poorly or not at all." Daniel Patrick Moynihan, *Secrecy: the American Experience* (New Haven & London: Yale University Press, 1998), p. 73.

National security and law enforcement

The need to maintain high levels of secrecy in national security matters is not the only barrier to accountability. Threats to national security pose an *intelligence* problem to governments charged with responsibility for maintaining public safety and promoting the national interest. Security and intelligence agencies collect information and assess such threats, employing intrusive surveillance and other extraordinary powers to do so. But security threats also pose a *law enforcement* problem, where criminal investigations and criminal prosecutions may be undertaken.

In Canada, prior to 1984, both security intelligence assessments and national security criminal investigations were the responsibility of the RCMP. Following the recommendations of the McDonald Commission of Inquiry in 1981[13], the government of Canada accepted that this combination of responsibilities in a single policing agency was inappropriate. Consequently in 1984, Parliament passed the *CSIS Act* creating CSIS as a security intelligence service with no powers of criminal investigation or prosecution, along with the *Security Offences Act*[14], which specifies law enforcement responsibilities for the RCMP regarding national security offences. This institutional division of responsibilities for national security is one that has long been practised in the United Kingdom, where the Security Service or MI-5 is separated from the Special Branch which undertakes criminal law enforcement. However, in the United States, the Federal Bureau of Investigation (FBI) continues to combine both security intelligence and national security law enforcement within the same agency.

Whatever the institutional arrangement, the distinction between security intelligence and law enforcement is important in determining appropriate mechanisms of accountability. In regard to law enforcement, there is in Canada the well-known principle of *police independence*, requiring an arm's-length relationship between external political control and decisions to initiate and/or to halt criminal investigations, as well as to prosecute.

[13] Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, 2nd Report, *Freedom and SecurityUnder the Law* (Ottawa: Minister of Supply & Services Canada, August 1981).
[14] R.S.C. 1985, c. S-7.

This has been widely accepted as a necessary safeguard against a government that might abuse its law enforcement powers by arbitrarily directing them at its opponents. In regard to security intelligence, direct political control of agencies engaged in sensitive national security threat assessments is generally regarded as not only desirable but necessary. In the absence of such control in the form of ministerial responsibility, security intelligence agencies with their extraordinary and intrusive powers might be seen as a potentially unchecked threat not only to the rights and liberties of citizens, but even to the elected government of the day. Where the two functions overlap, especially when they overlap within the same agency, there is inevitable tension between the need for both arm's length, and direct, control.

In 1984 Parliament prescribed different accountability mechanisms for CSIS and the RCMP, reflecting their different roles and the different principles of governance surrounding these roles. However, in practice, it may prove difficult to neatly separate national security law enforcement from security intelligence. For instance, a decision whether to undertake a criminal prosecution in a case of terrorism or espionage may require tradeoffs between the public interest in securing a conviction and the government's desire to maintain an undercover source or sources to gain a wider intelligence picture of the operations of a hostile organization or network. A prosecution against persons associated with a foreign state or a foreign non-state network may have repercussions for Canadian foreign policy. A decision to prosecute or not to prosecute a charitable organization for indirectly funding terrorist activities may have implications for the rights and privileges of individuals and identifiable groups in Canada, a legitimate political concern for democratic governments. This complexity and overlap of functions must be fully taken into account in devising an appropriate accountability mechanism for a law enforcement agency involved with national security issues.

Accountability *for what*?

Accountability may be used in reference to *propriety* or to *efficacy*. In practice, it is invariably in reference to both, but the two senses should be distinguished conceptually,

since they each entail somewhat different mechanisms of accountability.[15] Propriety refers to compliance with law and with ethical norms, both in relation to ends and to means. Are the goals of the security service appropriately framed in relation to the values of the society? Are the methods used ethically acceptable in light of the goals and of democratic values? Efficacy tends to focus on the relation of means to given ends: are they efficient and giving value for money?

Propriety issues are often directed in the first instance at national security agencies, reflecting concern at the potential for abuse of powers and at possible lack of democratic political control over agencies that operate in secret and may, when unchecked, threaten the rights of citizens and the rule of law. However, there is an opposite concern that is equally valid – that governments could misuse their national security agencies against their political opponents and against the legitimate activities of individuals or groups of which governments disapprove. Both kinds of potential abuse represent serious threats to the fundamental principles of a free society. Any effective accountability mechanism should take notice of potential abuse emanating from national security agencies acting beyond political control, and from governments abusing their national security powers for partisan advantage. Accountability in national security thus requires mechanisms that can balance these two different kinds of potential concerns.

Accountability *to whom*?

This leads to another dimension of accountability: *to whom* is the agency accountable? Broadly, there are five actors to whom forms of accountability may be directed: the *executive, judicial*, and *legislative* branches of government, special *public inquiries* called from time to time, and a more diffuse concept of the *public*.

Executive accountability relates mainly to efficacy: is the agency doing what the executive has asked it to do, and how effectively and efficiently? Judicial accountability

[15] R. Whitaker, 'The politics of security intelligence policy-making in Canada: 1 1970-1984', *Intelligence & National Security* 6:4 (1991), p. 650; R. Whitaker, 'Designing a balance between freedom and security', in Joseph F. Fletcher, ed., *Ideas in Action: Essays on Politics and Law in Honour of Peter Russell* (Toronto: University of Toronto Press, 1999), pp. 130-32.

relates almost exclusively to propriety: is the activity in compliance with law? Executive and judicial accountability are mainly of the control variety, since agencies must comply with cabinet directives and judicial rulings.

Legislative accountability is usually more mixed, combining efficacy and propriety concerns in shifting emphases depending on the issues and orientation of members. In a Westminster system, accountability to Parliament is, in practice, less control oriented than explanatory.

Much the same can be said for special public inquiries[16], the recommendations of which are not binding on governments, but advisory. Public inquiries on national security matters in Canada have been more likely to focus on propriety than on efficacy, since they have most often been called as a result of allegations of scandal of one kind or another. Inquiries' terms of reference may include efficacy issues as well. Occasionally, public inquiries are called primarily to address efficacy issues, as in the 9/11 Commission in the United States on why American intelligence failed to anticipate and prevent the September 11, 2001 terrorist attacks.

Accountability to the general public is also less predictable but has tended to focus more on propriety than efficacy, because there is less information available about the latter, and because the public, and especially the media (which *mediate* the public's perceptions of national security issues), respond to scandal and malfeasance more than to the complicated, arcane and often rather humdrum, details of the efficacy of the institutions and processes at work. If the media/public does perceive an efficacy issue, it is as often as not through the lens of a scandal. Accountability to the general public is a more diffuse concept than the other four types because there are few direct links between national security agencies and the public, other than public reporting on an annual or *ad hoc* basis by the agencies themselves, or indirectly through public reporting via the executive, legislative, judicial or special inquiry mechanisms. One issue that is specific to general

[16] Kent Roach, 'Canadian public inquiries and accountability' in Stenning, *Accountability for Criminal Justice*, *op.cit.*, pp. 268-93.

public accountability is access to information law and the ease or difficulty the media and public have in accessing information regarding national security matters. In Canada, the *Access to Information* and *Privacy* acts have been in effect since the mid-1980s, and have had some mixed success in permitting the diffusion of greater public information about the activities of national security agencies.

Accountability *by whom?*

It is easy to confuse the questions of accountability *to* and *by* whom, but while these sometimes overlap, they should be kept distinct. '*By* whom' refers to the specific body that actually conducts a review, which is different from the body to which it reports its conclusions. These will often both be in the same branch of government, but not always. For instance, the *CSIS Act* mandates two separate review bodies to report on CSIS. The Inspector General reports exclusively, and secretly, to the minister responsible, and thus offers a pure case of executive accountability, in both senses of 'by' and 'to'. However, the Security Intelligence Review Committee (SIRC) is constituted as an independent body that reports to the minister responsible, but also reports to Parliament, and with the publication of annual reports, to the public in general.

A parliamentary committee that reports to Parliament alone would be a pure case of parliamentary review, but a committee of parliamentarians that reports in the first instance to the prime minister (as in the United Kingdom) offers a mixed executive/parliamentary review. The office of the Auditor General, which conducts regular reviews of national security operations in the Canadian government is, although appointed by the executive, an independent officer of Parliament who reports to the Public Accounts Committee of the House of Commons.

There are a wide variety of specific accountability mechanisms that can be found in Canada and in other countries. Depending on the constitutional and political context, no single model can be seen as always and in every place the most appropriate. But when examining alternative mechanisms (the 'by whom'?) some general features should be considered. What is the appropriate degree of autonomy or independence, including

political or other pressures, that the review agency should have? Does the agency have sufficient resources to complete its task? Does it have access to persons and records commensurate with the requirements set for its review? Finally, does it possess sufficient legitimacy that its findings will be taken seriously and not simply as symbolic or a rubber stamp? These issues can be addressed by a variety of specific institutional mechanisms.

Accountability *of whom?*

The question of who is to be held accountable might seem obvious at first glance, but becomes more complicated on closer examination. In many cases, legislation specifies the body to be held accountable by review. This is the case with regard to the accountability mechanisms provided in the *CSIS Act*, where CSIS is the object or focus of the various mechanisms. The Director of CSIS is indicated as the officer responsible for the proper functioning of the Service, yet at the same time the Director answers to the Deputy Minister (formerly the Deputy Solicitor General, now the Deputy Minister for Public Safety and Emergency Preparedness), who in turn answers to the Minister, who is ultimately responsible and answerable for CSIS in Parliament. Clear lines of authority and ministerial responsibility were believed to be crucial to designing an effective accountability mechanism. However, in the case of the RCMP with its responsibilities for law enforcement and criminal investigation, the principle of police independence makes for more complicated lines of ministerial authority and responsibility.

Even with the ambiguities of responsibility, mechanisms of accountability that focus on a specified organization with its lines of authority have the virtue of clarity. Yet current trends in public management call this focus into question. The new public management stresses breaking down traditional departmental and organizational boundaries and building working partnerships across organizational boundaries, across jurisdictional boundaries, and even across the public and private sector divide, tending toward a new style of ‘governing without space’. “Public accountability in the traditional sense has been lost in a bewildering assortment of quasi-public or quasi-private agencies’, writes Donald Savoie.[17] He goes on to point out that accountability mechanisms have largely

[17] *Breaking the Bargain,* p. 244.

been designed with the old system of separate departments with clear boundaries around their responsibilities in mind. Thus, the trend to breaking down boundaries has "reduced accountability more than any shortcomings in the doctrine of ministerial responsibility."[18] This is a point that must be firmly addressed when contemplating any reform or improvement to existing accountability mechanisms.

Accountability *when?*

The question of the timing of accountability is crucially important, especially in sensitive national security matters. *Prior conditions*, constitutional,[19] legal, normative, or administrative, may be imposed upon agencies and officers specifying what they can and cannot, or should not, do. Forms of *ongoing supervision* may be imposed on their conduct. Finally, *ex post facto* review in the form of reports, financial audits, and evaluations provide the basis for public judgment on the performance of agencies and officials. Each of these have very different implications, for the agencies, and for the nature of accountability.

There is a distinction that may be drawn between accountability as *oversight* and as *review*. The two terms are sometimes used interchangeably with regard to national security.[20] However, greater precision in distinguishing the two usages is useful. As one observer has written, "'Oversight' means supervision, watchful care, management or control. 'Review' in contradistinction, means to view again, survey again, or take a retrospective view of events and activities that have already occurred. Accordingly, a

---

[18] *Ibid.,* p. 254.

[19] Laurence Lustgarten, 'Security services, constitutional structure, and varieties of accountability in Canada and Australia', in Stenning, ed., *Accountability for Criminal Justice*, *op. cit.*, pp. 162-84.

[20] In the CSIS Act, Part III is termed 'Review' in English and 'Surveillance' in French, the latter having more of a connotation of 'oversight' than review; similarly, the Security Intelligence *Review* Committee is called in French, Comité de *surveillance* des activités de renseignement de sécurité. This discrepancy has occasioned some misunderstanding among observers from time to time. In1990, SIRC announced that "with this annual report, we turn another small corner ourselves in hopes of ending a controversy over our past use of the term 'oversight' interchangeably with 'review' to describe our work. We now use the term 'review' only." They explained that the use of the term 'oversight' might be interpreted as invoking the wide powers of US congressional oversight committees, and thus "an attempt by us to stretch our mandate further than Parliament intended." SIRC, *Annual Report 1989-1990* (Ottawa: Minister of Supply & Services Canada, 1990), 1-2.

review process, strictly speaking, refers to an ex-post-facto process, where oversight suggests more of a watchdog function over ongoing activities of an agency."[21]

The Canadian government's 2004 consultation paper on a National Security Committee of Parliamentarians makes a clear distinction between the two terms, arguing that "confusion and crossed signals" have resulted when they are used interchangeably. This paper suggests that oversight, implying supervision, is "best understood by reference to the US system of government, where committees of the Congress have 'oversight' of federal agencies, meaning that the committees supervise these bodies, participating to a degree in their management and direction." In a Westminster parliamentary system like Canada's, oversight has been seen as the responsibility of ministers. Review on the other hand allows for an "independent assessment of the way in which the organization has performed", which makes in one sense for greater accountability.

Another way of looking at this issue is to return to the distinction between accountability as control, and as explanatory. The strong sense of oversight implies a degree of control. In the case of the US congressional oversight committees, there are elements of quasi-control vested in the committees, including a prior notification requirement for covert actions planned abroad. Parliamentary review in Westminster systems, on the other hand, does not vest any degree of control over executive action with parliamentarians outside cabinet. Review implies more of an explanatory than a controlling role. This need not, however, imply that *post hoc* review is merely passive or ineffective. The Auditor General's office produces informational audits of past performance, but it can promote compliance on the part of the executive due to the legitimacy and prestige of the office, as well as through its direct channel to parliament and to the general public.

Effective review can exercise indirect, if not direct control, by drawing attention to past mistakes and prompting remedial action. More importantly, effective review can alter the behaviour of those reviewed, in anticipation of future review. Internal control procedures

[21] Marina Caparini, 'Challenges of control and oversight of intelligence services in a liberal democracy', Geneva Centre for the Democratic Control of Armed Forces, Conference paper presented at the Workshop on Democratic and Parliamentary Oversight of Intelligence Services, Geneva, 2002.

may reflect the internalization of external review recommendations. In other words, focusing on review instead of oversight should not be taken as an admission that accountability is weak in Westminster systems. Rather, it is the preferred instrument of accountability in such systems.