

## Overview of Best Practice

### The Agency

#### Defining the Mandate

- ✓ The role of a security or intelligence agency should be clearly defined and limited to matters which should be specified in detail and involve serious threats to national security and the fabric of civil society;
- ✓ The concepts of threats to national security and the fabric of civil society should be legally specified;
- ✓ The territorial competence of a security or intelligence agency should be clearly defined and any powers to act outside the territory should be accompanied by safeguards;
- ✓ The tasks and powers of the agency within its mandate should be clearly defined in legislation, enacted by parliament;
- ✓ Especially in post-authoritarian states, it is important to have legal and institutional safeguards in place, preventing the misuse of security and intelligence against domestic political opponents.

#### Appointing the Director

- ✓ Legislation should establish the process for the appointment of the Director of a security or intelligence agency and any minimum qualifications or any factors which are disqualifications from office;
- ✓ The appointment should be open to scrutiny outside the executive, preferably in parliament;
- ✓ Preferably, the opposition in parliament should be involved in appointing the Director;
- ✓ Legislation should contain safeguards against improper pressure being applied on the Director and abuse of the office (for example provisions for security of tenure, subject to removal for wrongdoing);
- ✓ The criteria for appointment and dismissal should be clearly specified by the law;
- ✓ Preferably, more than one cabinet member should be involved in the process of appointing a Director, eg the head of state/prime minister and the relevant cabinet minister.

## Authorising the use of special powers

- ✓ It is a requirement of the rule of law that any special powers that the security or intelligence services possess or exercise must be grounded in legislation.
- ✓ The law should be clear, specific and also comprehensive, so that there is no incentive for an agency to resort to less regulated means;
- ✓ The principle of proportionality should be embedded in legislation governing the use and oversight of special powers;
- ✓ There should be controls against the misuse of special powers involving persons outside the agency, both before and after their use;
- ✓ All actions taken by security and intelligence services to fight terrorism should respect human rights and the principle of the rule of law. Whatever the acts of a person suspected or convicted of terrorist activities, intelligence services may never derogate from the right to life as guaranteed by the ECHR and the International Covenant of Civil and Political Rights (ICCPR);
- ✓ In order to safeguard against arbitrary use of special powers and violations of human rights, the agency's actions must be subject to appropriate supervision and review.

## Information and Files

- ✓ The legislative mandate of the security and intelligence agencies should limit the purposes and circumstances in which information may be gathered and files opened in respect of individuals to the lawful purposes of the agency;
- ✓ The law should also provide for effective controls on how long information may be retained, the use to which it may be put, and who may have access to it and shall ensure compliance with international data protection principles in the handling of disposal information. There should be audit processes including external independent personnel to ensure that such guidelines are adhered to;
- ✓ Security and intelligence agencies should not be exempted from domestic freedom of information and access to files legislation. Instead they should be permitted, where relevant, to take advantage of specific exceptions to disclosure principles referring to a limited concept of national security and related to the agency's mandate;
- ✓ The courts or whatever other independent mechanism is provided under the legislation should be free to determine, with appropriate access to sufficient data from the agency's files, that such exceptions have been correctly applied in any case brought by an individual complainant;
- ✓ Where information is received from an overseas or international agency, it should be held subject both to the controls applicable in the country of origin and those standards which apply under domestic law;
- ✓ Information should only be disclosed to foreign security services or armed forces or to an international agency if they undertake to hold, and use it subject to the same controls as apply in domestic law to the agency which is disclosing it (in addition to the laws that apply to the agency receiving it).

## **Internal Direction and Control of the Agency**

- ✓ Intelligence services should not be beyond the law. Therefore staff who suspect or become aware of illegal actions and orders within the services should be under a duty to report their suspicions;
- ✓ A codified practice should be in place which guarantees appropriate support and security for whistleblowers;
- ✓ Intelligence Services staff should be trained to a code of conduct which includes consideration of the ethical boundaries to their work. This training should be kept up to date and available to staff throughout their tenure;
- ✓ Internal administrative policies should be formalised with a clear legal status.
- ✓ Matters too detailed or sensitive to appear in legislation should be governed by formal internal administrative policies with a clear legal status.

## The Role of the Executive

### Ministerial Knowledge and the Control of Intelligence

- ✓ Intelligence legislation should contain two distinct rights of access: the right of the executive to relevant information in the hands of the agency and the right of the agency heads to have access to the respective minister;
- ✓ The Minister should be legally responsible for the formulation of policy on security and intelligence matters. He should also be legally entitled to receive agency reports at regular intervals as well as being legally responsible for the approval of matters of political sensitivity.

### Control over Covert Action

- ✓ All covert action shall be approved by the responsible member of the executive according to a legal framework approved by parliament. Regular reports shall be made;
- ✓ No action shall be taken or approved by any official as part of a covert action programme which would violate international human rights.

### International Co-operation

- ✓ It is essential that international cooperation should be properly authorised by ministers and should be subject to minimum safeguards to ensure compliance with domestic law and international legal obligations;
- ✓ Legal safeguards should be incorporated to prevent the use of intelligence sharing in a way that circumvents non-derogable human rights standards or controls in domestic law.

### Safeguards against Ministerial Abuse

- ✓ Intelligence legislation should include safeguards against ministerial abuse and the politicisation of intelligence services. Various possible safeguarding mechanisms are imaginable, such as the requirement that all ministerial instructions be put in writing and/or disclosed to an external review body as well as the ministerial requirement to brief the Leader of the Opposition;
- ✓ Intelligence Services should not take any action to further the interests of a political party;
- ✓ Intelligence Services should not be allowed to investigate acts of protest, advocacy or dissent that are part of the democratic process and in accordance with the law.

## The Role of Parliament

### The Mandate of Parliamentary Oversight Bodies

- ✓ Horizontal scope of the mandate: the entire intelligence community, including all ancillary departments and officials, should be covered by the mandate of one or more parliamentary oversight bodies;
- ✓ Vertical scope of the mandate: the mandate of a parliamentary oversight body might include some or all of the following (a) legality, (b) efficacy, (c) efficiency, (d) budgeting and accounting; (e) conformity with relevant human rights Conventions (f) policy/administrative aspects of the intelligence services;
- ✓ All six aspects mentioned above should be covered by either the parliamentary oversight body or other independent bodies of the state, eg national audit office, inspectors-general, ombudsman or court. Overlap should be avoided;
- ✓ The bigger an intelligence community is and the more different intelligence services are involved, the greater is the need for specialised parliamentary oversight (sub)committees;
- ✓ The mandate of a parliamentary oversight body should be clear and specific;
- ✓ The recommendations and reports of the parliamentary oversight body should be (a) published; (b) debated in parliament; (c) monitored with regard to its implementation by the government and intelligence community;
- ✓ The resources and legal powers at the disposal of the parliamentary oversight body should match the scope of its mandate.

### The Composition of a Parliamentary Oversight Body

- ✓ Parliamentary oversight bodies should be clearly 'owned' by parliament;
- ✓ Parliament should be responsible for appointing and, where necessary, removing members of a body exercising the oversight function in its name;
- ✓ Representation on parliamentary oversight bodies should be cross-party, preferably in accordance with the strengths of the political parties in parliament;
- ✓ Government ministers should be debarred from membership (and parliamentarians should be required to step down if they are appointed as ministers) or the independence of the committee will be compromised. The same applies to former members of agencies overseen;
- ✓ Committee members should have security of tenure at the pleasure of parliament itself, rather than the head of government;
- ✓ The chairman should be chosen by the parliament or by the committee itself, rather than appointed by the government.

## Vetting and Clearance of the Oversight Body

- ✓ Members of parliament should only be vetted if the committee's mandate includes dealing with operationally sensitive material;
- ✓ Where clearance is denied to members of parliament by the security and intelligence services, procedures should be established to deal with disputes authoritatively, giving the final decision to the parliament or its presidium;
- ✓ The criteria for vetting should be clear, public, consistent and robust in order to withstand democratic scrutiny.

## Parliamentary Powers to Obtain Information and Documents

- ✓ The oversight body should have the legal power to initiate investigations;
- ✓ Members of oversight bodies should have unrestricted access to all information which is necessary for executing their oversight tasks;
- ✓ The oversight body should have power to subpoena witnesses and to receive testimony under oath;
- ✓ Where relevant to the oversight body's remit, the executive should have responsibility for keeping the oversight body informed;
- ✓ The oversight body should take appropriate measures and steps in order to protect information from unauthorised disclosure;
- ✓ Disputes over access to information between the agencies and the oversight body should be referred in the last analysis to the Parliament itself.

## Reporting to Parliament

- ✓ Primary responsibility for the timing and form of the Parliamentary Committee's Report and any decision to publish evidence should lie within the committee itself;
- ✓ The committee should report to parliament at least yearly or as often as it deems necessary;
- ✓ The parliamentary oversight body should have the final word on whether it is necessary to remove material from a public report for security reasons;
- ✓ The government and the agencies should be given prior sight of the draft report so that representations about necessary security deletions can be made.

## Budget Control

- ✓ The oversight body should have access to all relevant budget documents, provided that safeguards are in place to avoid leaking of classified information;
- ✓ The oversight of the budget of the security and intelligence services should be governed by the same principles of good governance which regulate other activities of government. Exceptions should be regulated by law. From this

*Making Intelligence Accountable: Legal Standards and Best Practice*

point of view, the oversight of the budget should be a shared power between the appropriations committee and the intelligence oversight committee;

- ✓ Powerful parliaments should have the right to authorise the budget;
- ✓ Intelligence Agencies should only use funds for activities if those funds were specifically authorised by the legislative branch for that purpose;
- ✓ The intelligence services should not be allowed to transfer funds outside the agency without the authorisation of the legislature.

## The Role of External Review Bodies

### Resolving Citizens' Grievances

- ✓ 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 so 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 proceedings 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.

### Oversight of Agencies within the Administration by Independent Authorities

- ✓ 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;
- ✓ 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.



## **Independent Audit Offices**

- ✓ 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.

