Vetting and the Security Sector

10/2006

DCAF

Geneva Centre for the Democratic Control of Armed Forces

This document is part of the DCAF Backgrounder series, which provides practitioners with concise introductions to a variety of issues in the field of security sector governance and reform.

What is vetting?

Vetting is a process by which individuals are screened for access to rights or duties. Vetting in one form or another is carried out for practically all positions in government and business. For instance, whenever a job applicant is asked about their criminal background, this constitutes a form of vetting.

In the security sector, vetting tends to be much more rigorous and extensive. When properly conducted, it constitutes a vital part of the counterintelligence process.

Why is vetting necessary?

Vetting is necessary to exclude from public office individuals who represent a threat to the state because they:

- hold anti-constitutional views;
- are affiliated with terrorist groups, organised crime or political pressure groups; or
- are vulnerable to pressure, extortion or corruption.

Furthermore, vetting helps to:

- ensure the probity and honesty of staff and prevent fraud;
- protect VIPs, sensitive sites and classified information; and
- discourage inappropriate individuals from applying for security-related positions in the first place.

Who needs to be vetted?

Vetting is usually required for anyone that has access to sensitive information or sites, or that disposes of significant powers.

Candidates for the following positions are nearly always vetted:

- staff serving key members of the executive;
- members of the security forces (intelligence and security agencies, the military, national police and gendarmerie);
- staff of parliamentarians mandated with oversight of the national security apparatus;
- staff with physical access to sensitive sites; and
- non-governmental persons, such as employees of contractors or think tanks having access to classified information or providing services to the government related to national security.

In addition, some countries require the vetting of elected officials with access to sensitive information. Others assume that the public mandate of an elected official constitutes a sufficient level of trust to justify access to power and information. Germany, for instance, requires the vetting of parliamentarians on their defence and intelligence committees, while the United States does not (see the **DCAF Backgrounder** on Parliamentary Committees on Defence and Security).

Vetting is not only done at the time of recruitment. 'Aftercare', as it is sometimes called, is performed at regular intervals (usually at least every five or ten years), as well as anytime suspicions exist about an individual's reliability. Supervisors often receive training on how to recognise suspicious behaviour, and co-workers are encouraged to report any unusual activity or other reasons for concern. In addition, if the duties of a staff member change, managers must assess whether that individual still requires a security clearance. Some job changes may also require vetting for a higher security clearance.

Some countries may also require other governments to certify that their nationals have been properly vetted in the case of certain cooperative security-related activities, such as in international arms procurement and development. Such a process is generally codified in a memorandum of understanding or other agreements.

Who conducts vetting activities?

In most cases, the individual or department in charge of vetting is separate from the one entrusted with recruitment. There are essentially three different ways to organise vetting activities.

In most countries, the security or intelligence services or a specialized agency handles the bulk of national vetting tasks, while a few agencies conduct their own vetting activities. Such a centralised approach helps to ensure that:

- standardised vetting procedures are followed;
- individual agencies do not have to develop their own vetting capabilities, allowing them to concentrate on their core missions; and
- resource use is optimised by eliminating redundant capabilities.

Approaches to Vetting

Centralised – Central agency or unit performs vetting (or certain duties of vetting) for multiple services

Decentralised – Independent agencies or units perform vetting

Outsourced – Private businesses perform vetting (or certain duties of vetting)

However, agencies may resist a centralised approach in order to keep information on their own personnel secret and maintain control over their own vetting procedures and recruitment requirements.

In a few countries, each agency is responsible for its own vetting. In Switzerland's decentralised system, each federal or cantonal agency conducts its own vetting. When employees of government contractors are being vetted, the contracting agency is responsible.

Some countries outsource vetting tasks to private businesses in order to reduce costs. This usually involves activities such as credit and criminal record checks that extensively rely on data provided by or collected by private companies.

Most countries follow a mixture of these procedures. In Canada, for instance, all government vetting is performed by a single agency, the Canadian Security Intelligence Service, except for vetting for the Royal Canadian Mounted Police. In Sweden, the Security Police (SAPO) conduct most government vetting activities, including electronic database checks, while other agencies conduct additional vetting processes. The military, for example, administers psychological tests to officer candidates.

In the UK, the Defence Vetting Agency handles vetting for the armed services, MoD civilian staff, defence intelligence staff and defence contractors, as well as for sensitive private industry on a repayment basis. Five other agencies also perform vetting services, including for their own personnel: the Security Service, the external and signals intelligence agencies, the Foreign and Commonwealth Office and the Office of Civil Nuclear Security.

In a number of societies, for instance in many Middle Eastern countries, where access to key positions and sensitive information is regulated by family ties and tribal affiliations, there may be no formal vetting system in place. Even in such systems, however, screening of some individuals may be carried out by the intelligence services via more informal mechanisms.

In the US, two agencies conduct the bulk of the vetting, the FBI (for its own recruitment, for other federal agencies such as the White House, the Department of Justice, the Administrative Office of the U.S. Courts and certain House and Senate committees, as well as for state and local law enforcement officials that need access to restricted information) and the Office of Personnel Management (OPM) (for most other federal civilian agencies, sometimes in tandem with the Department of Defense). Other agencies, such as the State Department and the intelligence agencies, conduct vetting activities for their own personnel.

However, regardless of who is doing the vetting, most countries make efforts to ensure that vetting is standardised. In Germany and Switzerland, vetting guidelines are codified in law. In the US, these are mandated by presidential order. Regardless of the authority under which they are issued, they must ensure that standard procedures are followed throughout the government, and that democratic safeguards are in place to guard against malpractice.

What are some of the main vetting techniques?

While vetting processes vary from country to country, certain standard techniques are generally used.

Disclosure forms are often the first step of the vetting process, requiring the individual to submit the following kinds of information:

- full name and any prior names;
- employment history;
- residency, presence and activities abroad;
- financial status; and
- information on prior legal convictions or court proceedings.

In addition, disclosure forms usually include a 'catch-all' question asking whether any conflicts of interest exist and requiring the applicant to acknowledge that lying, misrepresentation of the truth or deliberate omission of information could constitute grounds for denial of employment or subsequent dismissal.

Electronic checks can include identity checks, which verify the authenticity of documents such as ID cards, passports, birth certificates, diplomas and other documents, and **background checks**, which may include the following:

- criminal and national security records, including foreign records, if appropriate;
- medical records, which may reveal that the candidate suffers from medical or psychological conditions that could have a bearing on the ability to handle sensitive information; and
- financial records of the subject and their family for signs of serious financial difficulty or irresponsibility that could make them vulnerable to inducement, as well as for unexplained wealth.

Subject interviews are one of the most common vetting techniques. Inquiries may include questions regarding details of the disclosure form, plus such factors as:

- family background,
- past experiences,
- health,
- personal life,
- relationships with nationals from certain countries,
- use of drugs and alcohol,
- affiliation with certain organisations,
- political views and
- hobbies.

Checking of references in writing or by telephone is usually mandatory, as well as (in important and highly sensitive cases) personal interviews of friends, teachers, acquaintances, neighbours and employers. In most cases, consent for these interviews must be granted by the individual being investigated before they are conducted. One of the most common causes of difficulty and delay in completing vetting inquiries is the non-availability or unsuitability of referees nominated by the candidate.

Other techniques that may be used include medical and psychological exams, polygraph interviews and fingerprinting.

How much vetting is necessary?

There are usually several different levels of sensitivity for information or sites. The greater access to classified information or sensitive physical locations a position provides, the stricter (and costlier) the vetting process is likely to be.

There is no magic formula for determining what information should be classified at which level. These are usually ranked in some order such as "classified", "secret" and "top secret". Vetting procedures for access to each level vary.

What human rights and governance challenges does vetting pose?

Invasion of privacy. By its very nature, vetting requires investigation into the private life of the individual beyond what would normally be permitted of the government. Approval should be obtained from the subject prior to the investigation. The only possible exceptions are military conscripts, whose consent may not be required for very limited vetting measures.

Abuses of power. The vetting process gives vetters enormous influence over the careers and lives of those whose credentials and character they subject to scrutiny. To prevent abuse by vetters,

- vetters must have undergone checks for the highest security clearances that they will vet for;
- vetters must be reinvestigated at regular intervals to prevent corruption, particularly as regards financial records;
- vetting staff should be generally representative of the population as a whole;
- subjects should have the right to see the results of the investigation; and
- subjects should have the right to appeal and request that inaccurate or irrelevant data be removed from their file.

Inappropriate vetting criteria. The choice of inappropriate criteria can result in the rejection of qualified applicants or the inclusion of too many unqualified applicants. Particularly difficult are criteria such as political affiliation, criminal records and past use of drugs and alcohol. These criteria vary from country to country. In democratic systems, political criteria should as a general rule aim only to exclude extremists that would seek to overthrow the government by non-democratic means. In most countries, limited prior drug use or minor criminal offences long in the past are not a bar to employment in the security sector.

Inefficiencies due to lack of data or faulty procedures. Vetting procedures can require enormous resources. The US OPM's 2006 rate schedule ranged from $80 for a simple national agency check to $3150 for a standard background investigation required for Top Secret clearance. Inefficient procedures can exacerbate these costs, or result in individuals having to wait an undue amount of time in order to receive their security clearances. To counter such problems, consideration should be given to whether there may be cost and efficiency benefits in

- standardising procedures across government,
- assigning certain vetting functions, such as record checks, to a centralised agency or privatising them, and
- simplifying access to data by use of national databases or standard research procedures.

Such challenges underline the necessity of vetting being governed by a robust legal framework for vetting. This should include the following elements:

- a national security statute that regulates the classification of information and vetting procedures necessary to gain access to each level;
- data protection laws that provide exemptions to the rules for processing personal information for vetting candidates: records should be held for a certain period after retirement or death before being destroyed; and

- human rights laws and non-discrimination statutes that do not prevent the screening of individuals working in positions related to national security for factors such as ethical belief, political opinion, psychiatric or medical illness, and national origin — all other relevant non-discrimination clauses should apply.

What are some of the particular challenges for transition and post-conflict countries?

Vetting in transition and post-conflict countries is intimately linked to issues of transitional justice. In these situations, vetting does not only involve clearing employees for access to information, but also screening individuals charged with offences such as undemocratic behaviour, human rights violations or war crimes. This process is commonly known as lustration.

Transition and post-conflict societies encounter many of the same problems that exist in consolidated democracies. In certain respects, however, the difficulties that are encountered with vetting may be more extreme:

- the legal framework is likely to be underdeveloped;
- institutions may be weak and fragmented;
- resources are likely to be insufficient to finance a vetting process that encompasses all echelons of the national security structure;
- data on individuals may not be available, as records may have been lost, destroyed or become subject to manipulation for political motives;
- there may be little or no political consensus;
- vetters may be corrupt or politically motivated; and
- there may be a lack of candidates that are both qualified and acceptable, making it necessary to downgrade vetting criteria and/or to hire or promote insufficiently experienced staff.

There are no sure-fire recipes for addressing challenges of this nature. However, it is essential for governments labouring under such circumstances to carry out a thorough analysis of the state's capacity for conducting vetting and to prioritise areas where reform and capacity-building is most critically required, particularly at the upper levels.

Further information

Canada, CSIS Security Screening
www.csis-scrs.gc.ca/en/priorities/security_screening.asp
www.csis-scrs.gc.ca/en/newsroom/backgrounders/backgrounder09.asp

New Zealand's Guidelines on Governmental Security. Chapter 5: Personnel Security
www.security.govt.nz/sigs/html/chapter5.html

United Kingdom, Defence Vetting Agency website
www.mod.uk/DefenceInternet/AboutDefence/Organisation/AgenciesOrganisations/DVA/

United Nations High Commissioner for Human Rights. Rule-of-Law Tools for Post-Conflict States. Vetting: an Operational Framework, 2006
www.ohchr.org/english/about/publications/docs/ruleoflaw-Vetting_en.pdf

United States, Adjudicative Guidelines for Determining Eligibility to Access to Classified Information, 2005
www.fas.org/sgp/isoo/guidelines.html

United States, Report of the Commission on Protecting and Reducing Government Secrecy, 1997
www.fas.org/sgp/library/moynihan/index.html

Procedures for screening individuals for access to restricted information

Switzerland

Levels of secrecy

Two
(*Classified, Secret*)

Types of vetting

Basic Security Check (for access to *Classified*)

- National and local agency check for convictions and current legal proceedings

Expanded Security Check (For access to *Secret*)

All of the above plus

- Disclosure form
- Check of financial and prosecutor's records in the cantons of residence
- If necessary, interviews with third parties, with the consent of the person under investigation

Expanded Security Check with Interview (for those denied the checks above, and for those who have regular access to important national security information)

- Third party interviews

Right to Appeal if Clearance Denied

Can request an investigation at the next highest level

After final rejection, right to a hearing, at which request can be made to:

- correct or delete incorrect data
- remove extraneous data from file
- eliminate unproved assumptions
- put indication of complaint on record

Germany

Levels of secrecy

Four
(*For Professional Use Only* - does not require formal vetting for access, *Classified, Secret, Top Secret*)

Types of vetting

Basic Security Check (for access to *Classified* and all workers in agencies dealing with national security)

- Disclosure form
- Review of all records from the Central Federal Register, criminal police, border police, and intelligence services
- If subject was born before 1970 and lived in the GDR or worked for its government, the relevant records are checked

Expanded Security Check (For access to *Secret*, to a large number of *Classified* documents, or when the appropriate authority does not believe that a basic check is sufficient)

All of the above plus

- Identity checks
- At discretion of the authority, checks of records of spouse or partner (with their consent)

Expanded Security Check with Investigation (for access to *Top Secret* information, a high number of *Secret* documents, the intelligence services and other organs so determined by the government)

- References and points of contact verified to confirm data and determine whether other reservations exist

Right to Appeal if Clearance Denied

Can request an investigation at the next highest level

In the event of a denial, the subject has the right to an appeal with a lawyer

Canada

Levels of secrecy

Three
(*Classified, Secret, Top Secret*)

Types of vetting

Basic Security Check (for access to *Classified* and *Secret*)

- Disclosure form
- Check of databases of Canadian Security and Intelligence Services (CSIS). Supplemented by interviews and field investigations if suspicious information is found

Field investigation includes CSIS records checks, interviews of third parties, local police checks and a subject interview

Right to Appeal if Clearance Denied

Can have reviewed decision by the Security Intelligence Review Committee and reapply for a clearance under certain circumstances

The DCAF Backgrounder Series
on Security Sector Governance and Reform

DCAF Backgrounders provide concise introductions to contemporary issues in security sector governance and reform. The series is designed for the use of practitioners and policymakers. Your feedback is encouraged. Please send comments and suggestions to backgrounders@dcaf.ch

This research for this Backgrounder was conducted by Fred Schreier and James Stocker, who also provided editorial assistance. David Law is the editor of the Backgrounder series.

Other Backgrounders are available at www.dcaf.ch/publications/backgrounders

Available Backgrounders

- Challenges for Intelligence
- Intelligence Services
- Military Ombudsmen
- Multiethnic Armed Forces
- National Security Policy
- Parliamentary Committees on Defence and Security
- Parliamentary Oversight of Intelligence Services
- Private Military Companies
- States of Emergency
- Parliaments & Defence Budgeting
- Parliaments & Security Sector Procurement
- Sending Troops Abroad
- Vetting and the Security Sector

Forthcoming Backgrounders

- Child Soldiers
- Military Justice Systems
- OSCE Code of Conduct
- Understanding Security Sector Reform