TRANSPARENCY INTERNATIONAL
Defence & Security

# SECRECY SHOULD NOT BE THE NORM IN RIGHT OF ACCESS TO INFORMATION IN THE DEFENCE SECTOR

**TI-DS Factsheet: Access to Information**

**The approach to transparency in government defence institutions needs to change. Currently, secrecy is often the norm and transparency is the exception. Instead, transparency should be the norm and secrecy the exception.**

Despite robust and widely agreed international and national anti-corruption and freedom of information legislation that governs public sectors, the defence sector remains secretive and lacking a fundamental level of transparency that is crucial to ensure accountability. Such legislation frequently contains national security exemptions that are vague, undefined or overreaching and provide defence institutions with a sweeping mandate to classify information by labelling it critical to national security.

The secretive nature of defence and a lack of transparency and access to information impairs civilian control of the security sector, hampers oversight bodies and increases corruption risks at all levels. It allows corruption to occur, unexposed and unaddressed, in the shadows.

To ensure an appropriate balance between transparency and genuine needs for secrecy, defence institutions should have in place rigorous and publicly available rules for withholding information. They should be accompanied by clear criteria and process for public interest and harm tests that can help balance genuine needs for secrecy with overall public interest, as set out in the Global Principles on National Security and the Right to Information (the Tshwane Principles).

The interest of preventing, investigating, or exposing corruption should be considered an overriding public interest, as corruption not only wastes public resources, but also seriously undermines the national security efforts of a country.


## Freedom of Information is a key element in the fight against corruption and for better governance

Access to information is one of the essential tools in combatting corruption and building institutional integrity. It enables external oversight of government by legislators, civil society and the media, increasing accountability of political decision-making and institutional practice. It enables informed participation of the public and civil society in public debates and development of policy and law. And it brings corruption risks – and actual incidents of corruption – to light, facilitating the push for accountability and reform.

### What is the Right to Information?

The right to information empowers citizens to obtain information held by public bodies albeit with limited exceptions. It encompasses a right to seek, receive and impart information, as well as an obligation on governments to publish information proactively.

## Mechanisms for public access to information in defence sectors currently lack effective implementation and leave defence sectors at risk of corruption

Findings from Transparency International Defence & Security (TI-DS)'s Government Defence Integrity Index (GDI), a research project that assesses how government defence institutions protect themselves against the risk of corruption, show that in most countries there is a long way to go to make mechanisms for accessing information from the defence sector effective. **Of the 86 countries assessed in the GDI 2020, almost half were found to be at high to critical risk of corruption in relation to their access to information regimes**. The legal frameworks for access to information, implementation guidelines, and effectiveness of practice at the institutional level are currently inadequate to ensure citizens' right to access information (source: country data for Q30 in GDI 2020).

Weaknesses in legal frameworks regulating access to information in defence expose countries to high levels of corruption risk as they reduce transparency and oversight of the sector. However, weaknesses in the implementation of these frameworks in practice presents even more significant risks. **The GDI data shows a clear implementation gap: even where legal frameworks are in place, most countries score less well in terms of applying these frameworks in practice.** The vast majority of countries fall well short of the good practice standard for implementation, whereby 'the public is able to access information regularly, within a reasonable timeline, and in detail'. Most were assessed as having at least some shortcomings in facilitating access to defence-related information to the public (for example, delays in access or key information missing), and in more than one in three of the countries assessed the public is rarely able to access information from the defence sector, if at all.

### Find out more

For more on current trends in defence sector governance and anti-corruption controls, including access to information, see the Government Defence Integrity Index (GDI) 2020

For more about the balance between national security and access to information, read about the Global Principles on National Security and the Right to Information (the Tshwane Principles)

Read about how some countries have grappled with the need to balance national security concerns with granting citizens the right to access information in TI-DS's Classified Information study

## States should ensure that clear guidance is in place, allowing for public access to information from defence institutions except in clearly defined circumstances

**No institution should be given a blanket exemption to responding to information requests—even in the name of national security**. While some information in the sector may need to remain classified, secrecy should be a well-founded exception, not a rule. Exceptions must be proportionate and necessary, and transparency should remain the default approach.

**Defence institutions should proactively make certain types of information available to the public and to independent oversight bodies**. This should include key information related to defence strategy, budgets, expenditure, audit reports and procurement data.

**Legislation and implementing guidelines in relation to access to information in the defence sector should clearly stipulate**: 1) how the public can access defence information; 2) what information is and is not available; 3) how classified information is categorised; 4) how the public can appeal those decisions; and 5) that there is an active, accessible, independent, external appeal or review body to review access to information decisions.

**Defence institutions should have clear and publicly available rules for withholding and classifying national security information**. This framework should also include additional safeguards, including time limitations on classification of information, and guidance on the application of tests balancing the public interest against the concrete harm of releasing specific information, ideally along the lines of the Global Principles on National Security and the Right to Information (the Tshwane Principles).

**Whistleblowers and journalists should not face retaliation** for seeking or publishing information, if the public interest in the information disclosed outweighs the public interest in secrecy.