TRANSPARENCY INTERNATIONAL
Defence & Security

CREATING ACCESS:
STRENGTHENING AND EXPANDING INFORMATION GOVERNANCE IN DEFENCE

This guide translates global standards on information disclosure into practical steps for the defence sector. It highlights how better laws, clearer practices, and stronger oversight can balance security with accountability, building on the findings of Unlocking Access (2024).

What's in it?

1 Review Critical Components of an ATI Regime

Understand the building blocks and implement, adapt, or expand:

1. Security classification schemes
2. Exemptions and state secrets
3. Balancing tests
4. Proactive disclosure
5. Implementation oversight

2 Answer Four Critical Questions

To highlight gaps and opportunities for strengthening information access:

1. What is the state of the legal framework governing access to information in national security?
2. What is the quality, accessibility, and relevance of publicly available information in national security?
3. How can information be used by civil society actors for accountability in the defence sector?
4. How can information access support state-society collaboration in the defence sector?

3 Apply Three Core Tools

A set of tools to generate a snapshot of ATI legal provisions and information availability, along with advocacy opportunities using global standards, multi-stakeholder partnerships, and national collaborative mechanisms:

1. Tshwane Principles: Legal Diagnostic
2. GDI: Institutional Mapping
3. Quick Reference for Action Planning

What is ATI?

A governance principle requiring governments to disclose information that is relevant to the public, ensuring it is accessible, accurate, and timely. In defence, ATI is vital for accountability, enabling scrutiny of finances, procurement, and policymaking, while balancing legitimate national security concerns.

How to use it?

The toolkit is designed for modular use. Readers can use a Scorecard Template to track progress.

Who should use it?

Anyone engaging with access to information in defence: governments, international organisations, oversight bodies, civil society.

Prepared by Stephanie Trapnell for Transparency International, Defence & Security | August 2025

ATI IN DEFENCE: KEY COMPONENTS

1. Security classification schemes

CHALLENGE

Security classification systems categorise information to protect it, pulling in the opposite direction of ATI. Governments typically assign classification levels based on the potential harm to national security from disclosure, thereby controlling access with specific security measures.

- **Classification of information is an administrative process** that occurs when information is produced during regular government operations. It happens independently of ATI mechanisms.
- **There is no international standard for maximum length of time** for records to be restricted in a security classification scheme.

HOW TO DO IT WELL

Governments with well-functioning security classification systems have a specific policy or framework for classifying and protecting information. A document is made available with both the justification and the method for restricting information access, thus allowing the public to understand how sensitive information is handled, how policy violations are addressed, and how civil society can advocate for revisions in the public interest.

Records should be automatically declassified (1) after expiration of a time limit, or (2) during a review process determining whether restrictions are still relevant or needed, or (3) following a trigger event (e.g., prompted by a public interest test).

ADAPTATION

When classification reform efforts meet resistance, collaboration with national archives can be a viable workaround. Their declassification mandates under archives law make them key partners for change.

EXPANSION

Even where classification systems are mature, weak review and accountability may facilitate over-classification. Recent reforms have adopted clearer, schema-based classification.

PRACTICAL CONSIDERATIONS

Elements of security classification

Information classification is the process of categorising information based on three factors:

1. **Sensitivity:** The level of sensitivity of an information is determined using classification policies and schema developed by an official government entity;
2. **Risk:** The likelihood of harm that could result from the unauthorised disclosure of the information, and the severity of its potential impact.
3. **Protection:** The level of protection required to keep the information secure, while granting access to a limited and designated group of people.

2. Exemptions and state secrets

CHALLENGE

Many countries over-restrict the release of national-security information. ATI or procurement frameworks relay on expansive, vague exemptions that act as blanket bans, and state-secret statutes prohibit and criminalise disclosure, and override other laws.

- **Transparency in defence is a balance between state secrecy and the public's right to know.** Often, keeping information secret is a legitimate way to protect national security interests, or in the case of procurement processes, the trade secrets of defence companies (e.g., new or advancing technologies).

- **The Tshwane Principles** (or the Global Principles on National Security and the Right to Information) identify which classes of information may be withheld in the national interest and when an overriding public interest requires disclosure. They are non-binding but set specific, internationally agreed guidelines.

HOW TO DO IT WELL

Exemptions to ATI should reflect legitimate national security interests as identified by the Tshwane Principles. Even in well-established ATI systems, legal reform will be necessary as contexts change, priorities shift, and technology advances.

ADAPTATION

In contexts where legal reform is not feasible, or legal initiatives are stalled, other avenues are possible:

- Continued advocacy in favour of disclosure with government officials and parliamentarians is critical to maintaining focus on needed reforms.
- Proactive disclosure might be an avenue to information access, albeit limited, in cases with unclear ATI mandates.
- Collaboration with oversight entities (e.g., information commissioners, ombudsmen) is important for sustaining support for legal reform.

EXPANSION

Countries with well-developed ATI laws and policies can publish good-practice guides drawn from experience in successful reforms, outlining how specific exemptions work and how balancing tests are applied in practice.

SECRECY IN THE NATIONAL INTEREST

Ongoing defence plans, operations, and capabilities

The production, capabilities, and use of weapons systems and other military systems

The operation, sources, and methods of intelligence services

Measures to safeguard the territory of the state, critical infrastructure, or critical national institutions against threats of force

Information on national security matters supplied by a foreign state with express expectation of confidentiality

DISCLOSURE IN THE PUBLIC INTEREST

Violations of international human rights and humanitarian law

Safeguards for the right to liberty and security of person, the prevention of torture and other ill-treatment and the right to life

Decisions to use military force or acquire weapons of mass destruction

Legal framework and procedures for authorising surveillance and use of collected material

Financial information

Public health, public safety, or the environment

Structures and powers of government

Accountability concerning constitutional and statutory violations and other abuses of power

3. Balancing tests

CHALLENGE

Under well-formulated ATI laws, when requests are made for protected information, a "public interest test" or "balancing test" is triggered, requiring authorities to establish the potential *harm* of disclosing protected information and then weigh it against the *public interest* in its disclosure.

- **Protected information** is outlined in the exemptions section of ATI or state secret laws.
- **Security classification should not automatically determine whether information is disclosed or restricted.** It is rather a factor to be considered in a balancing test.
- **ATI exemptions are subject to balancing tests**, while security classifications are subject to other types of administrative reviews.

HOW TO DO IT WELL

Balancing tests are administered by ministry and department officials, and require legal expertise, familiarity with ATI frameworks, and designated authority over sensitive and restricted defence information. These decisions fall outside legislative authority but should be subject to appeal before an independent authority and the judiciary.

ADAPTATION

When the government bureaucracy cannot conduct balancing tests due to instability, lack of expertise, or other challenges, proactive disclosure is an alternative.

EXPANSION

ATI systems with established balancing tests should consider regularly analysing and publishing decision outcomes to identify material for declassification or proactive release and to indicate when security-classification policy needs updating.

PRACTICAL CONSIDERATIONS

Weighing factors in a public interest test

Depending on a country's political and economic context, and the government's priorities, the definition of public interest can vary, and will change over time.

Factors that may **favour** disclosure, when the information:

- Contributes to the debate on a matter of public importance
- Enhances scrutiny of public decision-making and expenditure of public funds
- Addresses a public authority's performance of its regulatory functions
- Involves the handling of complaints by public authorities
- Exposes wrongdoing, inefficiency, or unfairness
- Allows individuals to refute allegations against them
- Protects against danger to public health or safety

Factors that may weigh **against** disclosure include:

- Likelihood of damage to security or international relations
- Likelihood of damage to integrity or viability of decision-making processes, or the ability of public bodies to perform their functions effectively (e.g. conducting investigation)
- Preserving the privacy of individuals and confidences

Factors that should be irrelevant to the consideration of public interest:

- Information might be misunderstood; or is highly technical in nature
- Disclosure may result in embarrassment to the government or to public officials

4. Proactive disclosure

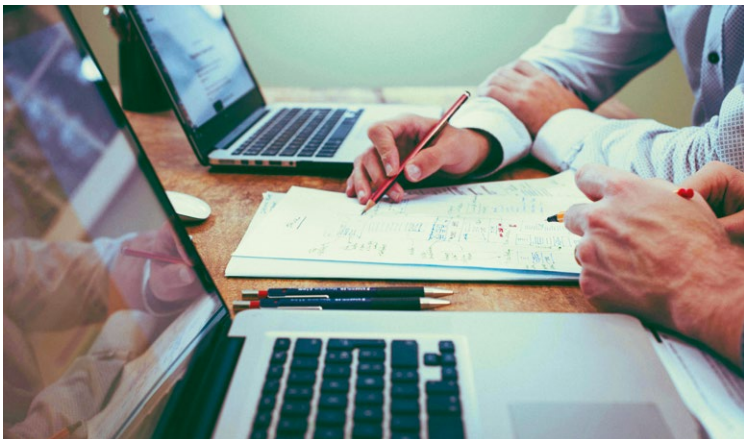
CHALLENGE

Processing information requests may generate a considerable amount of work for government entities. One way to eliminate the need to process information requests is the regular, proactive release of information that generates a high level of interest.

Information is identified for proactive release as part of an information management process, especially through an internal review of highly requested records**.**

HOW TO DO IT WELL

Proactive disclosure should be built into technology and information management reforms, and enabled by record digitisation and online portals. Many governments have created simple online platforms for disseminating information about defence activities, providing access to publication schemes, strategies, business plans, financial declarations, salaries, and machine-readable datasets.



ADAPTATION

Where disclosure mandates are unclear or information management weak, direct engagement with individual ministries can deliver small but meaningful wins while broader legal/administrative reforms proceed—e.g., discussions with senior MoD officials can identify public-interest categories for proactive disclosure, including:

- Budgets, income, expenditures, audit reports, and procurement, or specific aspects of each of these documents (if agreement on entire categories is unattainable).
- Information about military allowances and basic needs provision (e.g., housing, transportation, clothing, food)
- Information relevant for public health, public safety, and the environment, or critical for maintaining order and protecting lives.

EXPANSION

ATI systems with proactive disclosure mandates risk overwhelming the public with information that cannot be identified, analysed or accessed easily. Information inventories, user-friendly portals, and machine-readable files are essential for ensuring that information is found and used appropriately.

5. Implementation oversight

CHALLENGE

A dedicated oversight body is vital to realising ATI in defence, and to guide government entities on legal interpretation and the rollout of administrative reforms.

- **ATI oversight bodies may have binding powers,** which may compel disclosure and lead to the imposition of penalties. These entities often rule on appeals to information denials.
- **ATI oversight bodies may have non-binding powers,** which encourage cooperation and persuasion. These entities provide dispute resolution services as an alternative to litigation.

HOW TO DO IT WELL

ATI oversight bodies—typically information commissioners or ombudsmen—must be legally empowered and independent. In defence, effective oversight means continuous support to ministries on ATI implementation, with consistent, coherent guidance, as ATI often triggers major reforms in information management.

PRACTICAL CONSIDERATIONS

The problem of ATI enforcement in national security

Parliaments, executive branches, and other institutions can pressure departments that withhold information, but they rarely enforce rules. Without an ATI oversight body with enforcement powers, courts can compel disclosure on appeal, but proceedings may take months or years, and even empowered oversight bodies may struggle when national-security claims are raised. Cooperative implementation—discussion, consultation, joint planning, guidance, and review—usually reduces the need for enforcement and builds trust. Collaboration with civil society and private firms can also indentify bottlenecks, convene expert advice, and support consultations and training.

WHERE TO START: FOUR CRITICAL QUESTIONS

ANALYSE GAPS

1 What is the state of the legal framework governing access to information in national security?

Identify whether access to information is required by law

Are governments legally required to disclose information about national security activities and institutions? This question captures the legal obstacles to disclosure and the international agreements shaping national access to information.

This gap analysis covers the categories of information that should be disclosed according to the Tshwane Principles and highlights areas of potential legal reform.

TOOL **Tshwane Principles**

---

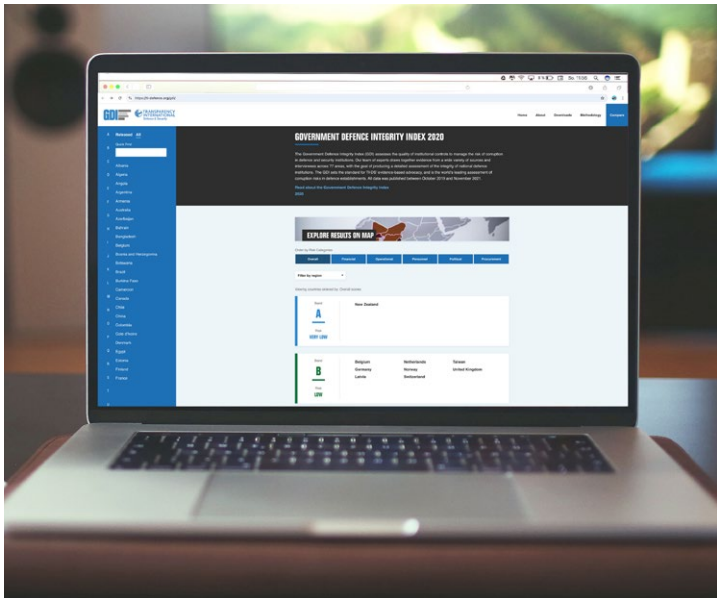
2 What is the quality, accessibility, and relevance of publicly available information in national security?

Assess access to national security information in practice

Is information about the national security apparatus being disclosed? How is it restricted in practice, possibly in violation of legal obligations? These questions also apply to any kind of national security information, including the information categories within the Tshwane Principles.

The Institutional Mapping Tool is based on transparency indicators from the Government Defence Integrity Index (GDI). Results from the analysis highlight areas for potential reforms in ATI implementation, related to national security generally and the defence sector specifically.

TOOL **GDI**



USE INFORMATION FOR ACCOUNTABILITY & ENGAGEMENT

3 How can civil society actors use information for accountability in the defence sector?

Civil society actors can use defence-related information for accountability purposes, including:

- **Research and analysis:** conduct research to identify corruption risks, analyse the effectiveness of ATI measures, and develop evidence-based policy recommendations.
- **Advocacy and lobbying:** engage with policymakers, government officials, and other stakeholders to promote legal and policy changes and strengthen access to information mechanisms.
- **Public awareness campaigns:** launch public awareness campaigns to educate citizens about national security, promote transparency and information access, and mobilise around ATI efforts.
- **Monitoring and evaluation:** monitor the implementation of ATI measures, assess their effectiveness, and provide feedback to governments and other stakeholders, on specific aspects of defence governance, including:
  - **Defence spending**—budget analyses, comparison of budget vs expenditure reports, analysis of annual reports from MoD.
  - **Defence income**—reviews of annual reports from military-owned businesses, investment vehicles, pension funds, and tracking of asset disposals.
  - **Defence industry relations**—comparison of financial disclosures by public officials and lobbying registers and records to identify conflicts of interests with organisations or individuals.
  - **Defence procurement**—tracking of contract suppliers, amounts, contract modifications, and deliverables, to determine how money is spent and whether it has resulted in appropriate services and products.

4 How can information access support state-society collaboration in defence?

Promote collaborative engagement with defence actors

How can civil society engage with defence actors in ways that strengthen the democratic governance of the defence sector?

Opportunities for engagement may include:

- **Providing inputs to policymaking,** including defence strategies, white papers, and systematic reviews, to ensure that policies align with societal values and priorities.
- **Providing inputs to administrative planning processes,** including acquisition processes and annual budgets, to allow for discussion of social and economic impacts.
- **Establishing collaborative models for policing and local security,** to ensure that initiatives respect communities values and build trust.
- **Establishing collaborative forums with MOD officials** for discussion of national priorities and reform processes, to help deliberations about the key components of an ATI regime.

THE ATI IN DEFENCE TOOLKIT

1 Tshwane Principles: Legal Diagnostic

Each of the categories in the table below (and any sub-categories) can be evaluated as:

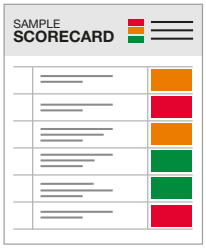
1. Must be disclosed
2. No requirement for disclosure or withholding
3. Restricted from public access

For each category, note the relevant laws and any global standards, conventions, or agreements the country has ratified or accepted.

Categories of national security information that serve the public interest and should be disclosed to the public
Violations of international human rights and humanitarian law
Safeguards for the rights to life right, to liberty and security of person, and the prevention of torture and other ill-treatments
Structures and powers of government
Decisions to use military force or acquire weapons of mass destruction
Legal frameworks and procedures for authorising surveillance and use of collected material
Financial information
Accountability concerning constitutional and statutory violations and other abuses of power
Public health, public safety, or the environment

The results of this tool can be displayed in a short scorecard, indicating the status of the legal framework with a colour code:

Red	Specifically restricted
Yellow/Amber	Not specifically to be disclosed nor specifically restricted
Green	Specifically required to be disclosed



Sub-categories can also be added to distinguish between different kinds of information:

1. Public health, safety, and environment can be broken down into three sub-categories.
2. Specific safeguards can be added regarding liberty and prevention of torture.
3. Specific anti-corruption provisions can be listed that apply to national security actors.

2 GDI: Institutional Mapping

How to determine the extent of access to defence-related information? The Government Defence Integrity Index (GDI) identifies the information that is critical for monitoring and accountability in the defence sector and the questions we should ask about each of them.

1. Which government body produces the information?
2. Is the information proactively released?
3. Where is it proactively released?
4. Is it released only by request?
5. Is it released in an appropriate format? (e.g., machine-readable data)
6. Is it released within an appropriate timeline?
7. Is it released without excessive omissions?
8. Did civil society provide inputs or participate in consultations?
9. What are the primary obstacles to access?

Defence-related information critical for monitoring and accountability in defence

National security strategy or defence white paper

Acquisition planning process

Notice of potential purchases

Notice of actual purchases

Defence budgets

Defence expenditures

Arms imports and exports

Public-private partnerships

Financial disclosure (income and assets)

Conflicts of interest

Contracting of private military and security companies (PMSCs)

Corruption prosecutions

Audit reports

Defence contracting – procurement

- Tenders
- Awards
- Suppliers
- Modifications to contracts
- Business integrity compliance
- Agents and intermediaries

Lobbying

- Lobbyist registration
- Public official reporting

Defence income

- Military-owned enterprises
- Beneficial ownership of private firms
- Investment funds
- Military involvement in natural resources
- Infrastructure projects
- Asset disposals

Bilateral and multilateral agreements

- Financing packages
- Offset agreements
- Security assistance

3 Action Planning

This guide equips civil society to drive change—through advocacy, research, and collaboration—to strengthen access to information in national security and defence. A basic action plan includes:

1. Understand the **Key Components of an ATI Regime** that matter for accessing information on national security topics.
2. Start with the **Four Critical Questions** to identify gaps and opportunities.
3. Apply the **Core Tools** to assess and build a picture of ATI in your context.
4. Use the **Scorecard Template** to colour-code progress for dissemination of findings.
5. Prioritise **Financial Transparency** for early wins: budgets, actual spending, defence income, procurement, audit reports.
6. Adapt to **National Context** and expand as appropriate.
   a. Identify internal and external stakeholders
   b. Collaborate on solutions with local actors, regional actors, government, private firms, and international organisations

- Consider engaging with international groups that specialise in freedom of expression to better understand how laws can be reformed: Article 19, International Center for Not-For-Profit Law, and IFEX, among others.
- Consider engaging with multistakeholder partnerships and global initiatives that focus on financial transparency: Open Contracting Partnership, Open Ownership, and International Budget Partnership.
- Consider engaging with the Open Government Partnership multistakeholder forum in your country to develop action plan commitments on ATI in national security and the defence sector.

Transparency International Defence & Security
10 Queen Street Place
London
EC4R 1BE

ti-defence.org
twitter.com/@TI_Defence

Transparency International UK
Registered charity number 1112842
Company number 2903386