Transparency International Anti-Corruption Helpdesk Answer

Best practices in civilian oversight and whistleblower protection in the armed forces

Author: Jessie Bullock, tihelpdesk@transparency.org
Reviewer: Matthew Jenkins, Transparency International
Date: 06 March 2019

Whistleblowing in the armed forces is mostly seen in terms of national security exemptions to whistleblower protection, on which there is a great deal of literature (see OECD 2014). However, there are specificities to the security forces that merit greater attention to ensure that whistleblowers are afforded sufficient opportunities and protection to report wrongdoing. Effective civilian oversight and whistleblowing channels in the security services are crucial, not only to identify corruption, abuse and other malfeasance but to protect legitimate national security interests from being damaged by uncontrolled leaks of sensitive information to outsiders.

Query

Please provide an overview of best practices for civilian oversight and control mechanisms of armed forces. In particular, please consider whistleblower protection measures that apply to members of the armed forces.

Contents

Main points

— There are tensions between protecting national security and transparency that make whistleblowing in the security sector riskier than in other sectors.

— There should be at least one oversight institution that is independent of the security sector and the executive that can receive whistleblower disclosures.

— Employees need clear protocols for internal and external reporting and rules for how to report sensitive information.

— The disclosures need to be investigated, acted on, and the whistleblower protected from employer reprisal.

Overview of civilian oversight of armed forces

Civilian oversight of the armed forces and whistleblower protection has been a topic of renewed global interest within the last decade, sparked by the Manning and Snowden revelations of US wartime and surveillance practices. The core issue that sets civilian oversight of the security sector apart from oversight in other sectors of government is national security. This has implications for when, how and whom whistleblowers should contact if they suspect wrongdoing.

There is a tension between protecting legitimate national security interests and exposing information about government wrongdoing that make civilian oversight more complicated in the security sector. The stakes are high for oversight and accountability for all players at this level: on one hand, whistleblowers within the security sector subject themselves to a great deal of legal and personal risk, while on the other, states argue that reckless disclosure of classified information could jeopardise national security.

For this reason, there are often legal exceptions for matters of national security in the text of whistleblower protection laws (OECD 2014). The protections afforded to some civil servants are not the same as to those in the security sector. Moreover, reporting policies in the security services may have a more formalised protocol; in some countries, security personnel must report internally first before turning to external oversight bodies to quality for whistleblower protection (DCAF 2012).

Countries and international bodies that have attempted to improve how whistleblower protection laws apply to the security sector tend to focus on the security sector as a whole, of which the armed forces are just one part. A narrow definition of the security sector typically includes “the armed

forces, paramilitary forces, gendarmeries, intelligence and security services, and law enforcement bodies such as border protection agencies and police forces" (DCAF 2013). This is important to keep in mind for institutional design of oversight mechanisms, as many of the accountability institutions are tasked with investigating or overseeing not only the armed forces but also a range of other law enforcement bodies.

This Helpdesk Answer outlines best practices for establishing civilian oversight that apply to members of the armed forces, paying close attention to the reporting, protection and enforcement mechanisms throughout the whistleblowing process.

International law

There are few international legal instruments that provide broad guidance related to civilian oversight and whistleblower protection in the armed forces. Moreover, there are no legally binding international treaties on this subject. Most of the guiding principles proposed by international bodies focus on the oversight of surveillance and data collection by intelligence institutions within the security sector. Though non-binding, the United Nations Compilation of Good Practices on Intelligence Agencies and their Oversight[1] (DCAF 2010) was one of the main documents to make recommendations on oversight of the intelligence sector and the security sector's compliance with the law, effectiveness and efficiency, finances, and administrative practices (DCAF 2010). The report identified 35 best practices for intelligence oversight, which either fell under the category of: i) legal basis; ii) oversight and accountability; iii) substantive human rights compliance; or iv) issues related to specific functions of intelligence agencies. These practices that apply to oversight, which are mainly focused on legal and institutional reform or setting a high international benchmark, are explained in next section.

Following the Snowden revelations, the United Nations special rapporteur on human rights and counter-terrorism issued a report encouraging member countries to adopt independent oversight bodies to oversee surveillance agencies and to adopt a process to address any violations of online privacy rights (UN 2014). The UN High Commissioner for Human Rights advocated for a separate security sector oversight agency or court that included "public interest advocacy positions" (UNHCHR 2014). The Centre for Democratic Control of the Armed Forces created a list of questions that governments can review when evaluating their existing institutions to see if they conform with the aforementioned principles (CIDS 2015).

One of the more influential non-binding international legal instruments is the Tshwane Principles (Global Principles on National Security and the Right to Information), initiated in 2013 by the Open Society Justice Initiative (Open Society Foundations 2013). These principles were created by more than 500 civil society experts and have been notably influential in European oversight of the security sector (PACE 2013). The Tshwane Principles focus on accountability and oversight of the security sector's access to information, and are some of the first sets of principles to recommend policies for informal oversight of the security sector by civil society, the media or NGOs. The most notable principles advocate for disclosure of information that is of high public interest (Principle 10), broad protections for whistleblowers, even those that were not employees (Principles 45, 46, 47), and that there should be no exemptions for public disclosure requirements, even for intelligence agencies (Principle 5).

The recommendations from this initiative trickled down to recommendations made by the Parliamentary Assembly of the Council of Europe (PACE) on parliamentary oversight of the security sector in Europe (PACE 2013). The recommendations were endorsed by the Council of Europe and later adopted by the European Parliament (Council of Europe 2015).

Domestic law

There is much more variation in domestic oversight of the security sector because of the sizeable differences in domestic political institutions. Different models of civilian oversight

[1] Hereafter: UN Compilation.

and whistleblower protection in the armed forces can be categorised into three primary groups:

- internal executive or security sector oversight
- independent public sector oversight
- and civil society oversight

Commonly, oversight of the security services is exercised by the executive branch of government, or even by a body within the security service itself. Given that senior positions within a state's security apparatus are typically appointed by and take their orders from the executive, the security services are rarely fully independent of the executive.[2] In this model, channels of domestic oversight can include control and reporting mechanisms within the armed forces that are separate from an officer's direct supervisor, whistleblowing reporting bodies within the security sector, and sometimes commissioners appointed by the executive who are tasked with reviewing practices within the security sector (Council of Europe 2015).

These internal oversight channels are generally preferred by the security services themselves, as they retain a high degree of control over the identification and management of alleged wrongdoing. While the probability of a national security secret being revealed is lower than where whistleblowers report wrongdoing to outsiders, such as the media, the chance of inaction or even cover-up is likely higher. Additional independent oversight from legislative or judicial bodies can thus provide an opportunity for more robust control of the security forces.

In fact, some countries operate a second oversight model, which involves the legislature or, less commonly, the judiciary. Legislative oversight bodies may have the mandate to investigate multiple aspects of the security sector, such as human rights practices, surveillance policy, budget and administration. These organs typically take the form of a parliamentary committee, but in some settings, the legislature may appoint an independent commissioner or external review body.

The ability to investigate the security sector and the democratic legitimacy of the committee members may make investigation or audit results more credible to an external audience. In addition, these channels may afford better protection to whistleblowers themselves by establishing procedures for reporting wrongdoing outside of the armed forces.

The Council of Europe (2015) states that, while judicial oversight is useful as a nominally independent check on executive power, it should be considered to complement rather than replace legislative oversight (Council of Europe 2015). There are a few reasons for this: judicial efficacy depends on the independence of individual judges, the expertise of individual judges, their propensity to be deferent to the executive, fear that judges may "rubber stamp" decisions regarding national security and because there are few ex-post oversight bodies over judicial decisions due to separation of powers (UNHCHR 2014; Council of Europe 2015). Judicial authorisation for warrants or subpoenas are some of "the best safeguards for human rights", and should be deployed if other institutions fail, but case law is not a replacement for well-designed policy.

Lastly, there are opportunities for civil society to monitor the security sector and protect whistleblowers. Non-governmental actors and investigative media outlets can play a vital role in monitoring the operations of a state's security organs and demanding accountability where wrongdoing is found to have occurred. As shown in both the Manning and Snowden revelations, media outlets may be the first organisations a whistleblower reaches out to. This is especially likely to be the case where whistleblowers have little confidence that their concerns will be effectively redressed via internal channels, or fear retribution. In addition to reporting, investigating and advocacy activities, civil society organisations may have the opportunity to sit on government appointed independent commissions and assist government bodies in policymaking regarding oversight and whistleblower protection.

[2] Of course, in parliamentary systems, the executive in power will be not be entirely independent of the legislature, but the relationship is not a direct reporting one like the relationship between security sector and the executive.

Frontier of whistleblower protection

The frontier of whistleblower protection includes multiple channels that involve all three domestic groups:

- oversight from within the security sector or executive
- oversight from independent legislative bodies
- principles for engaging with civil society institutions

Unambiguous legislation is essential to provide whistleblowers with clear guidance on where to disclose reported wrongdoing and to properly inform them of the protections, risks and enforcement mechanisms available. This includes clear definitions of what does and does not constitute whistleblowing, what is the mandate and domain of these institutions, and what individuals should do and expect if they want to report.

Experts highlight the importance of establishing reporting mechanisms and protections outside of the specific branch of the armed forces or security services to maintain credibility in the independence of the oversight body and reassure potential whistleblowers that they will be protected upon making their disclosure. The UN Compilation states:

> "It is good practice for this multilevel system of oversight to include at least one institution that is fully independent of both the intelligence services and the political executive. This approach ensures that there is a separation of powers in the oversight of intelligence service; the institutions that commission, undertake and receive the outputs of intelligence activities and not the only institutions that oversee these activities" (DCAF 2010, 17).

There is no one-size-fits-all model for which oversight institutions work best, since each government has its own unique institutions and security threats. Thus far, the most common channels appear to be legislative oversight bodies and independent commissions, which are either appointed by the legislature, executive or sometimes both. Legislative oversight bodies have been said to have "the ultimate 'democratic legitimacy', as elected individuals oversee security services" (TI Georgia 2018, p. 27). Their oversight is key because the security sector uses a lot of financial resources, and the legislature should have the power to make sure spending is efficient and policies are implemented correctly (CIDS 2016). Independent commissions or ombudsmen also seem to be on the rise – 16 of 28 EU member states had established this type of oversight body by 2017 (TI Georgia 2018).

Best practices for civilian oversight and whistleblower protection of armed forces

Transparency International advanced the International Principles for Whistleblower Legislation in 2013 (Transparency International 2013). Many of the principles that apply to whistleblowing more broadly are relevant and useful for whistleblowing in the security sector, but civilian oversight in the security sector entails heightened risks in terms of the content of the disclosure and possible state retaliation. The one principle related to security, Principle 19, states that "special procedures and safeguards for reporting that take into account the sensitive nature of the subject matter may be adopted in order to promote successful internal follow-up and resolution, and to prevent unnecessary external exposure" (Transparency International 2013).

The following best practices should be considered when:

- drafting legislation and adopting policies to strengthen civilian oversight structures of the armed forces
- defining the action of whistleblowing in the security sector
- managing whistleblowing reporting, protection and enforcement structures

Civilian oversight structures

Due to the tension between exposing critical information on national security and uncovering government wrongdoing, it is important for governments to have oversight institutions that are independent of the security sector and provide

reporting procedures. These bodies fall under the second model mentioned above as, unlike the executive branch, they do not have direct supervisory powers over the armed forces. These institutions can include the legislature or legislative committees, ombuds institutions, national human rights or transparency commissions, appointed oversight bodies or the judiciary (TI Georgia 2018). Several UN Compilation practices confirm that this is consistent with their best practices: they advocate for the importance of establishing an oversight body that is independent of the executive and security sector (Practices 6) which can conduct its own investigations (Practice 7), has broad access to information (Practice 25) and can examine information sent to foreign entities (Practice 35).

The need for independent oversight institutions in the security sector is paramount. In a US congressional hearing on the status of whistleblowing, a special counsel said, "I'd say that unless you're in a position to retire or are independently wealthy, don't do it. Don't put your head up because it will get blown off" (DCAF 2013, p.70). Given that the potential costs for whistleblowing in the security sector are often even greater than whistleblowing in civilian life, oversight institutions in this sector should prioritise being as explicit as possible and creating many channels for whistleblowers to come forward.

Public sector oversight bodies that are independent from the security sector and do not have direct supervisory power over potential whistleblowers are well placed to manage the delicate balance between the need to rectify potential government wrongdoing and protect whistleblowers while also protecting core national security interests.

There are a number of reasons that countries should take proactive steps to establish independent bodies with a mandate to oversee the security forces.

First, it sends a credible signal to the public and potential whistleblowers that wrongdoing, corruption or other abuses by security forces is taken seriously and will be investigated responsibly. Independent oversight bodies in both Japan and Latvia, two highly ranked countries in Transparency International Defence and Security Programme's report on the quality of legislative oversight, made their reports and recommendations open to the public to show their commitment to the recommendations (TI Defence and Security 2013). Japan's independent board of audit made the defence spending report publicly available and Latvia made their auditor general's office report on military funds for training personnel public. Both parliaments used these reports in forming committees and looking at policy changes or possible improvements to defence spending.

Second, external reporting channels are likely to afford potential whistleblowers greater protection. A well-designed oversight institution will have a clear protocol on how they will protect the whistleblower and handle the information disclosed, as well as investigate the potential wrongdoing. UN Compilation practices advocate for an independent agency for individuals to bring and resolves disputes, for a well specified protocol for how members of the security sector can report complaints (DCAF 2010, practices 9, 10, 18)

Third, where governments provide clear, independent and accessible channels to report suspected wrongdoing to state institutions, this may reduce the risk that a conscientious whistleblower with nowhere else to turn leaks sensitive security information to the press. UN Compilation practice 8 advocates for oversight institutions to "take all necessary measures to protect classified information and personal data … during the course of their work" (DCAF 2010, 10).

Germany's parliamentary control panel

The parliamentary control panel in Germany, established in 2009, is a legislative committee that oversees all federal security services, which includes their finances, policies and internal administration (EU FRA 2015). It is one of the most comprehensive legislative oversight bodies of

the security sector and includes detailed procedures on oversight, handling whistleblowing disclosures and investigative protocol. The mandate of this committee is extensive: it is tasked with reviewing internal reports from security sector agencies, investigating possible malfeasance and holding hearings.

This committee has established a few measures that can be viewed as good practices:

- Access to information: the members on this committee may access electronic or written information from all members of the security services, intelligence agencies or other branches of the federal government for review. If not granted access, they have a mandate to reach out to the judiciary to request assistance in obtaining information (TI Georgia 2018).

- Proactive disclosure of changes in the security sector: the Parliamentary Control of Federal Intelligence Services Law[3], which regulates the panel, requires security sector agencies to proactively report the following to the committee (TI Georgia 2018: 29):
    a) notable changes to Germany's foreign and domestic security situation
    b) internal administrative developments with substantial ramifications for the pursuit of the services' mandate
    c) singular events that are subject to political discussions or public reporting

- Investigate complaints: whistleblowers within the security sector can disclose complaints to this committee, which has the mandate and resources to investigate them. Between 2015 and 2017, the committee received 65 complaints about the security sector, 40 of which were about surveillance. The committee forwarded the more serious complaints to the G10 Commission, Germany's intelligence sector oversight body (EU FRA 2017). The G10 is an independent oversight body appointed by parliament, whose investigative and oversight powers are protected by a constitutional amendment.

Definition of whistleblowing

The ways that policymakers define the action of whistleblowing and the type of information it includes has important consequences for whistleblowing in the security sector. Even before arriving at a definition of whistleblowing, however, it is recommended that countries have a clear definition of the security sector's role, legal mandate, powers and competencies under national law, compliance with the constitution and international human rights law, and extent or limitations of their role in accordance with the constitution and international human rights law. Practices 1-5 of the UN Compilation advocates establishing a legal basis for these (DCAF 2010). The limitations of the security sector's reach, especially with regard to discrimination, targeting and human rights are further elaborated in practices 11-17 (DCAF 2010). Having a clear legal precedent of the role and mandate of security sector institutions could make it easier downstream in adjudicating whether or not these institutions are acting within their mandate or not.

In drafting domestic policy, experts recommend adopting a broad definition of a whistleblower and the act of whistleblowing (Transparency International 2013; DCAF 2013). Definitions typically state that "whistleblowing is the disclosure or reporting of wrongdoing", where wrongdoing may range from corruption and violence to environmental crime and even actions to cover up other acts of wrongdoing. By extension, a whistleblower is any public or private sector individual who is privy to this information and discloses it at their own risk, including but not limited to employees (Transparency International 2013).

[3] Full text of the law is found here: http://www.gesetze-im-internet.de/pkgrg/BJNR234610009.html

The third component of the definition, and most salient with regards to the security sector, is the threshold of "reasonable belief of wrongdoing". In other words, for the whistleblower to be protected by the oversight institutions in place, this reasonable belief must be present (Transparency International 2013).

There are a few best practices about "reasonable belief of wrongdoing" that are related to a whistleblower's motive and evidence (DCAF 2012, DCAF 2013).

First, some states have argued that the whistleblower's motive matters, and that only if a complaint is lodged in good faith should the whistleblower be protected by all resources available (DCAF 2012).

A policy that would ultimately provide more protection for whistleblowers, however, would clarify that motive is irrelevant if the disclosure indeed shows government wrongdoing, as mandating a good faith motive to each disclosure can lead to over-litigating (Public Concern at Work 2010). In fact, where a whistleblower's motive is open to attack by the authorities, this can be used to divert attention from the nature of the reported wrongdoing itself. This became apparent during the Manning trials, where prosecutors argued that Manning intended to harm the United States military and weaken national security (The Guardian 2013).

Second, the level of evidence required to make a disclosure should also be specified by domestic law. Most states use the language "honest and reasonable belief" to describe the level of proof or evidence necessary to classify a disclosure as whistleblowing (DCAF 2013).

Drawing from legislation in Australia, South Korea and the UK, experts argue that "honest and reasonable belief" is the appropriate level of specificity for whistleblowing in the security sector, as demanding higher levels of proof may encourage whistleblowers to commit illicit acts or leak information to outsiders (DCAF 2013). In addition, where the burden of proof is high, a whistleblower's efforts to collect sufficient evidence could tip off potential wrongdoers and lead them to destroy evidence. When drafting whistleblowing regulations, policymakers should maintain this "reasonable belief" standard of evidence for the security services and armed forces, rather than grant them exceptions. For example, if an employee of the security sector suspects malfeasance within their agency but is not certain, they should not violate a data collection law to collect more evidence to make their case stronger. One way to operationalise this could be for the policy to explicitly say that the burden of collecting extra proof is on the independent investigative oversight institution, not on the whistleblower (especially if it would cause them to break the law).

Reporting procedures

Reporting procedures for whistleblowing should detail the process and recipient of the disclosure so potential whistleblowers know who to turn to and how disclose their information.

Reporting lines and protocols will vary according to the type of oversight. The literature is clear that no single reporting channel is better than the other; rather, it emphasises the importance of multiple independent channels existing in the same country and the importance of not applying a one-size-fits-all model to all countries.

Where the oversight function is exercised by a direct supervisor, or an institution belonging to the executive branch, reporting procedures will differ from systems in which whistleblowers are entitled to make disclosures to a parliamentary committee or independent ombudsman.

Different still is a tiered reporting system, where whistleblowers must bring complaints to different channels in a specific order (DCAF 2012). Across these different reporting channels, the biggest differences will be the person hearing the complaint's relationship to the whistleblower, the investigative powers vis-à-vis the agency being complained about, and the possible retributive powers (DCAF 2012; DCAF 2013).

In all cases, however, best practices entail an unambiguous reporting procedure where the complaint process and reporting hierarchy is outlined clearly. This is consistent with practice 19 of the UN Compilation (DCAF 2010). The following examples are proactive steps that some countries

have taken to facilitate whistleblowing in the security sector at multiple levels of government:

- **Visibility of reporting channels**. Reporting channels must be made "visible", both internally within a given organisation and externally to relevant external and independent oversight bodies. Where a member of the armed forces wishes to blow the whistle, there should be at least one option to disclose malfeasance outside of their unit (DCAF 2013). Dissemination efforts are an important means of promoting all available channels among members of the security forces. Australia's security sector issues print and online information about whistleblowing reporting channels to employees, described more below.
- **Outline expectations for reporting at different channels**. In the UK, legislators have outlined a "tiered" approach to reporting, whereby different levels of severity of alleged wrongdoing correspond to different reporting bodies and different tiers of protection the whistleblower is afforded (Banisar 2011). This is another reason why there should be visibility and variety in reporting channels, because disclosures may range from minor malfeasance to classified information, and a whistleblower should be well informed about the risk they are exposed to and the protection they are entitled to (OECD 2014).
- **Anonymity and confidentiality**. Many countries have laws that protect the identity of whistleblowers and prohibit oversight bodies from releasing whistleblowers' identities. Given the sensitive nature of security sector disclosures, best practices seem to be to protect the identity until the whistleblower gives consent to disclose. There are laws punishing the disclosure of a whistleblower's identity without their consent in the US, Australia, Sweden and South Korea (OECD 2014). In Italy, a whistleblower's identity is one of the only things that cannot be obtained by a freedom of information request (OECD 2014). To preserve anonymity in the initial disclosure if whistleblowers are hesitant to come forward, some countries have implemented and had success with anonymous or independent hotlines to report (Banisar 2011).
- **Investigations**. There needs to be clear information available for whistleblowers on what to expect about their disclosure, if the body they reported to will investigate their report or will pass it along to another investigative body, and what the possible consequences of the investigation are. Some countries, such as Australia, have created a structure to monitor the progress of investigations as they are reported online.

Australia's Defence Whistleblower Scheme

Reporting is clear and structured in Australia's internal Defence Whistleblower Scheme. There are multiple ways that whistleblowers can choose to file a complaint within the security sector: there is a 24-hour hotline employees can call, they can see an investigator personally, or can write their complaint on a portal on the defence ministry's intranet. They can access information about these options in print or online materials that explains how to file each type of complaint and addresses questions such as identity protection, investigation follow-up and next steps (Transparency International 2016).

If the whistleblower does not want to make an internal disclosure, they can disclose their information to the Inspector General of Intelligence and Security, an independent, investigative body (OECD 2014). Australians are not required to report first to the internal structure and then, if referred or if desired, to the inspector general. The clarity of reporting structures built into the internal disclosure system, however, likely was designed to encourage internal reporting.

Protection mechanisms

There are two elements of whistleblower protection that are essential in the security sector. First, there is an urgent need to protect whistleblowers from retaliation by peers or superiors. Second, if and

where reprisals do occur, there needs to be reliable means of providing recourse.

Given the precedent for prosecuting and persecuting whistleblowers where disclosures are alleged to have threatened national security interests, adherence to these two principles is essential.

Firstly, whistleblower protections from reprisal range in scope. In New Zealand's case, the piece of legislation regulating whistleblowing in the security services states (New Zealand 1996):

> "where any employee of an intelligence and security agency brings any matter to the attention of the Inspector General [for Intelligence and Security], that employee shall not be subjected by the intelligence and security agency to any penalty or discriminatory treatment of any kind in relation to his or her employment by reason only of having brought that matter to the attention of the Inspector-General [unless done in bad faith]."

The United States' CIA has a similarly broad whistleblower law and encourages recourse if the whistleblower suffers damages (DCAF 2012). However, the CIA's complaint handling body, the inspector general, states that, during investigations, "Failure on the part of any employee or contractor to cooperate with the Inspector General shall be grounds for appropriate administrative actions by the Director, to include loss of employment or the termination of an existing contractual relationship" (DCAF 2012, p 199). These sanctions from the oversight body offer far fewer protections to whistleblowers.

Another example of the variation in protection is the sequencing of reporting, and the consequences that may have. Some countries have tiered reporting systems, where they have a strict protocol to whom a whistleblower must take their complaint to first, second and so on. In Canada, security sector employees are supposed to make their first disclosure to an internal channel to be eligible for protection (DCAF 2012). It is more difficult to successfully defend himself or herself if the first disclosure they make is to an external channel, especially if they reveal classified or sensitive information (DCAF 2012).

Secondly, countries should proactively provide recourse where reprisals occur. Currently, few countries clearly specify sanctions that should be applied to those found to have retaliated against whistleblowers in the security sector (DCAF 2013). Regulations should state whether whistleblowers can seek recourse for retaliation in court, from independent tribunals or dispute resolution bodies, or if there is a civil settlement process (DCAF 2013).

Transparency International's Recommended Principles for Whistleblower Legislation argue that civil fines or, in extreme cases, jail time, may be appropriate reprisals (Transparency International 2013; DCAF 2013). The implementation of these measures varies widely from country to country. In Hungary, the punishment is a prison sentence of no more than two years, community service or a fine; in South Korea, it is no more than two years of prison or two million won; and there is no clear precedent in the United States (DCAF 2013 p. 81).

South Korean act on the protection of public interest whistleblowers

In 2011, South Korea issued a comprehensive list of all forms of reprisal that should be prohibited by employers.[4] The list includes: disciplinary action of any kind; being dismissed, suspended, demoted, harassed or intimidated; being transferred against their will; being refused transfer or promotion; changing terms of employment or retirement; being refused a reference or written a bad reference from the employer; being denied appointment to any employment, profession or office; being threatened with the above actions, or any other adverse treatment that is a result of whistleblowing (Republic of Korea 2011).

This comprehensive list extends broad protections to whistleblowers for many possible types of

[4] The full text of the bill is here: https://sherloc.unodc.org/cld/document/kor/2011/act_on_the_protection_of_public_interest_whistleblowers.html

reprisals they could face from colleagues or employers, but has one critical flaw. The wording of "protection of the public interest" does not specify if there are any national security exemptions or not. It has been criticised for not adding a "no loopholes" clause to encourage disclosures in the security sector (OECD 2014).

Other best practice protections that could be relevant specifically for the security sector include protections from: "retaliatory investigations to divert attention from the issues that the whistleblower is trying to expose; ordering psychiatric tests or examinations; conducting unlawful surveillance (particularly of an employee's communications with an independent oversight body); physical and emotional abuse and intimidation; and security clearance suspension or revocation" (DCAF 2013: 20).

Enforcement mechanisms

The central purpose of whistleblowing and the reason individuals subject themselves to the considerable risks involved is to address wrongdoing. Once identified, it is up to the oversight institutions, the institution that overreached and other institutions involved in the sector to correct the error and implement new or change existing policy.

DCAF recommends that the body charged with receiving reports of wrongdoings should be responsible for issuing a follow-up report on future actions taken and what, if anything, has been implemented by the agency in question (DCAF 2012). This is the case regardless of whether the oversight body in question is part of the armed forces, a legislative committee or an independent body such as an ombudsman. For each of these institutions, CIDS' needs analysis has sample questions they can ask themselves when thinking about institutional change (CIDS 2016).

Implementing routine reporting on follow-up of investigations and reforms is crucial to ensure that the changes flagged by a whistleblower are actually implemented. This speaks to the core tension between national security and transparency that is present in the armed services, since high levels of transparency may be counterproductive to the goals of the organisation.

The Netherlands' follow-up reports

The Netherlands' Review Committee on the Intelligence and Security Services (CTIVD) has established policies on how to handle reports based on whistleblower disclosures. They allow the agency accused of wrongdoing six weeks to comment on the whistleblower's disclosure, and if they fail to comply, the content will become public (DCAF 2012). Once the responsible minister comments within the specified timeframe, the CTIVD carries on with the investigation.

This sanction provides a strong incentive for security forces to comply with oversight agencies' investigations, as otherwise sensitive information will be published. It is a sensible compromise of setting a reasonable deadline but also agreeing to not disclose the possibly sensitive information from the agency in question.

Key players working on civilian oversight of armed forces

Centre for Democratic Control of the Armed Forces (DCAF)

The Centre for Democratic Control of the Armed Forces (DCAF) is an intergovernmental organisation that that conducts research and provides policy guidance to member states on improving security, rule of law and human rights protections within a democratic framework. There are 63 member states and DCAF also works with international actors (intergovernmental or non-governmental actors) in order to build knowledge and contribute to good policy in the security sector. In addition to numerous policy briefs and books cited in this Helpdesk Answer, they have developed online courses for security forces that are interested in democratic reform.

Centre for Integrity in the Defence Sector (CIDS)

The Centre for Integrity in the Defence Sector (CIDS) is an agency within the Norwegian Ministry

of Defence's Department of Management and Financial Governance. Their mission is to promote global integrity in the defence and security sector globally. They publish handbooks, guidance documents, sample policy and conduct training programmes for security professionals, in-country and internationally. They lead NATO's integrity-building initiative and have several sample policy documents, academic publications and training programmes available on their website.

Transparency International Defence and Security Programme (TI Defence)

Transparency International Defence and Security Programme is an international programme of Transparency International that advocates for greater transparency in the defence sector. The programme works with armed forces leadership, other government leaders and civil society to conduct workshops, roundtables and advise on policy action. They also produce reports on defence and corruption, accountability in the defence sector, conflict and insecurity, and corruption in the arms trade and with defence companies.

References

Banisar, D. 2011. "Whistleblowing: International Standards and Developments" in Sandoval, I. (editor), Corruption and Transparency: Debating the Frontiers between State, Market and Society, World Bank-Institute for Social Research, UNAM, Washington, D.C.

CIDS. 2015. *Criteria for Good Governance in the Defence Sector: International Standards and Principles*.

Council of Europe. 2015. *Democratic and Effective Oversight of National Security Services*.

DCAF. 2010. *United Nation Compilation of Good Practices on Intelligence Agencies and their Oversight*.

DCAF. 2012. *Overseeing Intelligence Services: A Toolkit.*

DCAF. 2013. *Whistleblowing in the Security Sector: Protection of Whistleblowers*.

European Union Agency for Fundamental Rights. 2015. *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU – Mapping Member States' legal frameworks*.

European Union Agency for Fundamental Rights. 2017. *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU – Volume II: Field Perspectives and Legal Update*.

Khemani, M. 2009. *The Protection of National Security Whistleblowers: Imperative but Impossible: A Critical Appraisal of the Scope and Adequacy of Whistleblower Protection Laws for National Security Whistleblowers*. Washington DC: Georgetown University Law Center.

New Zealand. 1996. *Inspector-General of Intelligence and Security Act*, Section 18.

Open Society Foundations. (2013). *Global Principles on National Security and the Right to information (Tshwane Principles)*.

OECD. 2014. *Revisiting Whistleblower Protection in OECD Countries: from Commitments to Effective Protection.*

PACE. 2013. *Parliamentary Assembly of the Council of Europe Resolution 1954 (2013), 2 October 2013.*

Public Concern at Work. 2010. *Where's Whistleblowing Now? 10 Years of Legal Protection for Whistleblowers.*

Republic of Korea. 2011. *Act on the Protection of Public Interest Whistleblowers.*

The Guardian. 2013, August 3. Bradley Manning leak has had chilling effect of US foreign policy, court hears. *The Guardian.*

The Netherlands. 2011. Review Committee on the Intelligence and Security Services (CTIVD), *Annual Report 2010–2011*, Chapter 4.

Transparency International. 2013. *International Principles for Whistleblower Legislation: Best Practices for Laws to Protect Whistleblowers and Support Whistleblowing in the Public Interest.*

Transparency International. 2016. *Building Integrity and Countering Corruption in Defence and Security.*

Transparency International Defence and Security Programme. 2016. *Watchdogs: Quality of Legislative Oversight of Defence in 82 Countries*.

Transparency International Georgia. 2018. *International Standards and Good Practices in the Governance and Oversight of Security Services.*

UN. 2014. *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, A/69/397.*

UNHCHR. 2014. *The Right to Privacy in the Digital Age. A/HRC/27/37, UN High Commissioner for Human Rights.*

TRANSPARENCY INTERNATIONAL
the global coalition against corruption

"Anti-Corruption Helpdesk Answers provide practitioners around the world with rapid on-demand briefings on corruption. Drawing on publicly available information, the briefings present an overview of a particular issue and do not necessarily reflect Transparency International's official position."

Transparency International
International Secretariat
Alt-Moabit 96
10559 Berlin
Germany

Phone: +49 - 30 - 34 38 200
Fax: +49 - 30 - 34 70 39 12

tihelpdesk@transparency.org
www.transparency.org

blog.transparency.org
facebook.com/transparencyinternational
twitter.com/anticorruption

Transparency International chapters can use the Helpdesk free.
Email us at ***tihelpdesk@transparency.org***