

Intelligence Oversight: Warrants, Committees and the Ban on Domestic Political Surveillance

October 2026

Series: Security-Sector Transition & Rule-of-Law Safeguards — research papers accompanying [the Security-Sector Transition & Rule-of-Law Safeguards working blueprint](#). **Paper S4.**

Working paper, draft for review. Forward design only; nothing here is settled policy.

1. The question

A democratic transition on the mainland would inherit intelligence services built to protect a ruling party rather than a constitutional order. What rules should govern intelligence collection from the first day, so that services can still detect real threats but permanently lose the power to watch citizens for their politics? Three instruments are examined: judicial warrants, standing oversight bodies, and a statutory ban on domestic political surveillance.

2. The hub position

The security-sector blueprint holds that military, police, intelligence and detention bodies must come under public law, courts, budgets and audit, and that the objective is "lawful national institutions, not a new party army" [1]. It keeps defense, policing, intelligence and detention as distinct functions, defines civilian control as control through law, budgets, courts and audit, and lists party-controlled intelligence and election interference as triggers for external review [1]. Detailed intelligence rules are left open. The institutional baseline records that no public oversight mechanism for PRC (Mainland) intelligence services is documented [2].

3. Evidence and comparative options

The starting point. The PRC (Mainland) National Intelligence Law, adopted by the NPC Standing Committee on 27 June 2017 and amended in 2018, obliges organizations and citizens to support, assist and cooperate with intelligence work (Art. 7) [3]. It permits technical reconnaissance measures after unspecified "strict approval formalities" (Art. 15), and relies on internal review and a citizen reporting channel (Arts. 19, 26, 27), with no court or legislative body named as overseer [3]. A transition starts from zero external oversight.

International baseline. The UN Special Rapporteur's 2010 compilation of good practices (A/HRC/14/46) is the leading standard [4]. Mandates should be narrow and set out in public law (Practice 2). Services may not promote the interests of any political, ethnic or social group (Practice 12), and Practice 13 states: "Intelligence services are prohibited from using their powers to target lawful political activity" [4]. Oversight should combine executive, parliamentary, judicial and specialized bodies, with at least one civilian institution independent of both the services and the executive and holding full access to information, officials and premises (Practices 6–7) [4]. Rights-limiting measures need external, often judicial, authorization (Practice 22); personal data may be kept only while strictly necessary (Practices 23–25); and individuals need a complaints body with binding powers (Practices 9–10) [4]. The Council of Europe's Venice Commission adopted its report on democratic oversight of the security services in 2007 and updated it in 2015 [5].

United States: oversight born of domestic abuse. The Senate's Church Committee (1975–76) documented FBI and NSA programs that monitored and disrupted domestic political groups, including COINTELPRO [6]. The result was a permanent Senate intelligence committee in 1976 and, in 1978, the Foreign Intelligence Surveillance Act with a court reviewing warrants [6]. Under FISA, a judge must find probable cause that the target is a foreign power or its agent, and a US person cannot be so treated "solely upon the basis of activities protected by the first amendment"; most orders against agents run at most 90 days [7]. A political-activity exclusion written into the warrant test is more enforceable than general neutrality language.

United Kingdom: committee plus judicial "double lock". Under the Justice and Security Act 2013, the Intelligence and Security Committee has nine parliamentarians appointed by each House after Prime Ministerial nomination and consultation with the Opposition, overseeing agency expenditure, administration, policy and operations [8]. The Prime Minister may exclude matters from its published reports, but each report must say whether anything was excluded [8]. Under the Investigatory Powers Act, a minister issues the most intrusive warrants, but they take effect only with a Judicial Commissioner's approval on necessity and proportionality [9].

Germany: standing panel and constitutional pressure. The Bundestag's Parliamentary Oversight Panel may demand detailed information from the federal government on intelligence activity, and a separate G 10 Commission decides whether restrictions on the privacy of communications are permissible [10]. In May 2020 the Federal Constitutional Court held that the foreign intelligence service is bound by fundamental rights even abroad, and required both a court-like body issuing binding decisions and an administrative body making random checks, each with its own budget and staff [11].

European human-rights law. In 2021 the European Court of Human Rights' Grand Chamber found the UK bulk-interception regime violated Articles 8 and 10, requiring "end-to-end safeguards" with independent authorization and review [12].

ROC (Taiwan): from presidential directive to statute. The National Security Bureau, created in 1955 by presidential directive, received a statutory basis only with its Organic Law promulgated on 30 December 1993 [13][14]. That law contains no neutrality clause [13]. The National Intelligence Services Act of 2005 added one: personnel may not hold party posts, recruit for political groups, or build party organizations inside agencies, and agency heads must report to Legislative Yuan committees each session [15]. In 2007 Judicial Yuan Interpretation No. 631 struck down a rule letting prosecutors issue their own surveillance warrants, holding that a neutral court should in principle review applications before surveillance begins [16].

Republic of Korea: neutrality is necessary but not sufficient. December 2020 amendments removed the National Intelligence Service's investigation powers over national-security offenses from 2024, banned illegal wiretapping and restated neutrality; Human Rights Watch warned that a broad counter-intelligence mandate could still enable domestic surveillance [17].

Spain: a dedicated warrant judge. Organic Law 2/2002 requires the intelligence service to obtain prior authorization from a Supreme Court magistrate for measures affecting the home or communications, decided within 72 hours (24 if urgent), with interception limited to three-month renewable periods [18].

Files after the fall. Germany's Stasi Records Act, passed by the Bundestag on 14 November 1991, created the legal framework for access to former secret-police records, now administered by the Federal Archives [19].

4. Recommended design

1. **Statutory existence.** No intelligence body operates except under a published statute; unlisted units are dissolved and their assets and records registered.
2. **Functional separation.** Foreign intelligence, counter-intelligence and criminal investigation sit in separate bodies; intelligence services hold no powers of arrest, detention or prosecution.

3. **Ban on domestic political surveillance.** No service may collect, retain or analyze information about any person or group because of lawful political opinion, party membership, religion, ethnicity, petitioning, journalism, assembly or association. No warrant may rest solely on such activity.
4. **Neutrality.** Personnel may not hold party or candidate posts, recruit for political groups, or maintain party organizations inside any agency. Breach is a dismissal offense and, where it affects an election, a criminal offense.
5. **Judicial warrants.** Interception, entry, location tracking, bulk data acquisition and equivalent measures require prior approval from a designated judge of the highest ordinary court on necessity and proportionality, for renewable terms of no more than 90 days. Urgent measures must be submitted within 24 hours or stop, and unlawfully obtained material is destroyed.
6. **Standing legislative committee.** The assembly elects an intelligence committee with an opposition chair or deputy, full access to classified information and premises, approval of classified budgets, and a right to be kept fully informed.
7. **Independent expert commission.** Judges and technical experts, with their own budget and staff, audit operations at random, receive whistleblower reports and publish an annual report stating what was withheld.
8. **Remedy.** Any person may complain to a tribunal with binding powers; targets are notified once notice no longer endangers an operation.
9. **Data retention.** Personal data are held only while strictly necessary and reviewed annually; deletion is supervised externally, and records relevant to legal proceedings are preserved.
10. **Legacy files.** Pre-transition surveillance files are frozen on day one, moved to an independent archive, and opened to the persons concerned and to courts under privacy safeguards.
11. **Sunset review.** Every intrusive power lapses after five years unless re-enacted after public review.

5. Open questions and risks

- **Interim period.** Before an elected assembly exists, who exercises committee functions? An interim panel of judges is one option, but it concentrates power in an unelected body.
- **Counter-intelligence creep.** As the Korean case shows, a broad counter-intelligence mandate can reopen domestic surveillance, so definitions must be tight [17].
- **File access versus privacy.** Opening legacy files serves truth and vetting but exposes third parties; the archive's access rules need careful design.
- **Capacity.** Warrant judges need technical literacy, or approval becomes rubber-stamping.
- **Foreign liaison.** Intelligence shared with foreign services may escape domestic safeguards; oversight must reach liaison arrangements.

6. Cross-links

- Hub: Security-Sector Transition & Rule-of-Law Safeguards: <https://freechina.live/governance-public-policy/third-republic-governance-blueprints/security-sector-transition-rule-of-law/>
- Command & Control: The PLA, PAP, Police & Intelligence (institutional baseline): <https://freechina.live/governance-public-policy/military-public-security-civilian-control/command-control-pla-pap-police-intelligence-baseline/>
- Domestic Security & Stability Maintenance: The Weiwen Apparatus: <https://freechina.live/governance-public-policy/military-public-security-civilian-control/domestic-security-stability-maintenance-weiwen/>
- Military, Public Security & Civilian Control: <https://freechina.live/governance-public-policy/military-public-security-civilian-control/>
- Transition Readiness methodology: <https://freechina.live/governance-public-policy/third-republic-governance-blueprints/transition-readiness-methodology/>
- Companion papers in this series: S1 *Civilian Command From Day One*; S2 *Vetting Without Purge*; S3 *Demobilizing the Stability-Maintenance Apparatus*.

Sources

1. <https://freechina.live/governance-public-policy/third-republic-governance-blueprints/security-sector-transition-rule-of-law/>
2. <https://freechina.live/governance-public-policy/military-public-security-civilian-control/command-control-pla-pap-police-intelligence-baseline/>
3. <https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/>
4. <https://www.right-docs.org/doc/a-hrc-14-46/>
5. <https://www.coe.int/en/web/venice-commission/-/cdl-ad-2015-010-e>
6. <https://www.senate.gov/about/powers-procedures/investigations/church-committee.htm>
7. <https://www.law.cornell.edu/uscode/text/50/1805>
8. <https://www.legislation.gov.uk/ukpga/2013/18/part/1>
9. <https://www.ipco.org.uk/what-we-do/the-double-lock>
10. <https://www.bundestag.de/en/committees/bodies/scrutiny>
11. <https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2020/bvg20-037.html>
12. <https://www.statewatch.org/media/2443/echr-bulk-surveillance-uk-bbw-judgment-pr-25-5-21.pdf>
13. <https://irp.fas.org/world/taiwan/nsbb2-1.htm>
14. <https://irp.fas.org/world/taiwan/nsb.htm>
15. <https://www.6laws.net/6law/LAW/國家情報工作法.htm>
16. <https://cons.judicial.gov.tw/download/download.aspx?id=337258>
17. <https://www.hrw.org/news/2020/12/22/south-korea-revise-intelligence-act-amendments>
18. <https://boe.es/boe/dias/2002/05/07/pdfs/A16439-16440.pdf>
19. <https://www.bundesarchiv.de/en/stasi-records-archive/legal-basis/>

In this series: [Civilian Command From Day One](#) · [Vetting Without Purge](#) · [Demobilizing the Stability-Maintenance Apparatus](#).

Working paper v1.0, published October 2026 as part of the Security-Sector Transition & Rule-of-Law Safeguards blueprint program. This paper will be updated as the evidence base develops.