

# Brief overview of intelligence and security oversight bodies in certain countries

*This overview contains information about some of the countries that have external, independent bodies that specialise in oversight of intelligence and security services.*

## Sweden

### **The Swedish Commission on Security and Integrity Protection (SIN)**

SIN was established in 2008 and oversees the Swedish law enforcement agencies, including the police and Swedish Security Service (Säpo). Among other things, SIN oversees the registration of personal data and use of covert coercive measures. The oversight body also oversees whether the Swedish Police and the Swedish Security Service comply with the prohibition against using intelligence from the National Defence Radio Establishment (FRA) to investigate crime.

The chair and deputy chair of SIN must have background as judges. The other members are proposed by the party groups in the Swedish Parliament (the Riksdag). The members are appointed by the government.

SIN can also receive requests from individuals of whether they have been subjected to unlawful surveillance or registration. SIN shall notify the individual that the check has been carried out.

Other interesting facts about SIN:

- SIN publishes its findings on its website on a continuous basis.
- SIN regularly gives advice to the government in the form of consultation submissions on new bills.
- SIN can inform the prosecuting authority of any criminal acts the Commission may become aware of, or the body can report the matter to the Chancellor of Justice if it believes that individuals may be entitled to compensation.

[Link to SINs website here](#)

### **The Swedish Foreign Intelligence Inspectorate (SIUN)**

SIUN is the Swedish oversight body that oversees foreign intelligence activities. SIUN's remit includes overseeing the *Military Intelligence and Security Service* (MUST), the SIGINT intelligence service the *National Defence Radio Establishment* (FRA), the Swedish Defence Research Agency and the Swedish Defence Materiel Administration.

SIUN was established in 2009 and reports to the government.

The chair and deputy chair of SIUN have a legal background. The five other members are chosen for their political backgrounds as former or present members of the Riksdag.

Like SIN, individuals can 'request a check' from SIUN, but this only applies to FRA's signal intelligence activities. In such cases, SIUN can check whether FRA has acted in a manner that warrants criticism.

SIUN also has the power to demand that information collection is stopped and information deleted.

[Link to SIUN's website here](#)

Sweden has a specialist court, the **Swedish Foreign Intelligence Court** (*Försvarsunderrättelsedomstolen*), which determines which signal intelligence measures FRA is permitted to implement.

[Link to the specialist court's website here](#)

The Swedish Authority for Privacy Protection has a role in the oversight of the country's intelligence and security services, as do the Chancellor of Justice and the Parliamentary Ombudsmen. These oversight bodies also accept complaints from individuals.

## Denmark

**The Danish Intelligence Oversight Board (TET)** oversees the Danish domestic and foreign intelligence services (DSIS and DDIS), the Danish Centre for Cyber Security (CFCS), and the PNR Unit of the Danish National Police.

TET oversees that the services' collection, processing, deletion, and disclosure of personal data complies with the relevant regulations. While TET is tasked with oversight of the legality of the services handling of personal data, TET does not oversee how the services use sources and agents.

TET was established in 2014 and is composed of five non-political members and a secretariat of approximately 10 employees. TET is an independent authority appointed by the government and its yearly reports are made public.

TET has direct access to all relevant systems and can demand the services to provide any information that is relevant for the oversight, no matter where on the services' premises the information is located.

When handling complaints, TET may order the intelligence services to delete information. In contrast, TET has no authority to order the intelligence services to implement specific measures when it performs its regular ex post oversight.

However, TET may issue recommendations to the services. If the service does not comply with the recommendations, the service must notify TET and immediately submit the matter to the relevant minister for decision. If the minister decides not to follow the recommendations of TET, the Government must notify the Parliamentary Committee for the Intelligence Services.

[Link to TET's website here](#)

### **The Parliamentary Committee for the Intelligence Services, the Danish Folketing**

This parliamentary committee is highly secretive about its business, and all members are bound by a duty of total secrecy about what they learn. Five politicians from five parties in the Folketing make up this committee.

[Link to the Committee's website here](#)

The Danish Data Protection Agency also plays a role in overseeing the creation of databases and information security in the services.

## Finland

### **The Intelligence Ombudsman of Finland**

This independent oversight body for intelligence and security services was established in 2019.

Finland has two intelligence services – the Finnish Security and Intelligence Service (SUPO) and the military intelligence authorities (Defence Command Intelligence Division and Finnish Defence Intelligence Agency). Unlike the Scandinavian countries, Finland doesn't draw a clear distinction between foreign and domestic intelligence. Instead, a distinction is drawn between civil and military intelligence.

The Intelligence Ombudsman oversees both services and investigates complaints and requests for examination filed by citizens. The Intelligence Ombudsman has extensive rights of access and inspection, and the power to make binding decisions – for example to stop the use of methods the ombudsman deems to be unlawful or not in compliance with a court order.

The Intelligence Ombudsman is appointed by the government, but it is defined as autonomous and independent.

The Intelligence Ombudsman has the right to be present in court in cases concerning the intelligence and security services' requests for permission to use intelligence methods. The Ombudsman also has the right to speak in court and to file a complaint against the court's decision.

Moreover, the Intelligence Ombudsman has a consultative role in connection with new legislation relating to the intelligence and security services.

[Link to the Ombudsman's website here](#)

### **The Intelligence Oversight Committee of the Finnish Parliament**

This parliamentary oversight committee was established in 2019.

The Committee's main tasks are to monitor the appropriateness of intelligence activities and evaluate the priorities of those activities. The Committee also promotes and follows the implementation of human rights in the field of intelligence.

The Committee shall receive answers to any questions it may ask, and it may request that the Intelligence Ombudsman carries out specific inspections.

The Committee is responsible for considering reports submitted by the Intelligence Ombudsman.

*In Finland the Office of the Data Protection Ombudsman has a role in the oversight of the Intelligence and security services' personal data processing.*

## Germany

The German oversight system consists of a number of different oversight bodies and oversight committees. The German system is also distinctive in that the country does not just have intelligence services at the federal level. The different states of Germany also have their own intelligence services as well as state oversight bodies and data protection authorities.

The **G 10 Commission** conducts both ex ante and ex post oversight. Some members have political backgrounds while others are experts in relevant fields. There are also G 10 commissions at state level.

The members of the G 10 Commission are appointed by the **Parliamentary Oversight Panel**, whose members are all members of the German Parliament, the Bundestag. They also have a role in both ex ante and ex post oversight.

The German oversight bodies' right of access to sensitive information is somewhat less extensive than is the case for many other European oversight bodies.

The **German Federal Commissioner for Data Protection and Freedom of Information** (BfDI) has the broadest ex post oversight mandate in relation to how the services comply with the data protection regulations. They can inspect the services and consider complaints from persons who believe that the services have unlawfully stored their personal data. The BfDI must also be consulted before any new intelligence system is put into operation.

A new oversight body for German foreign intelligence, the Independent Control Council (**Unabhängige Kontrollrat**) was established in 2022 after the Federal Constitutional Court concluded that oversight of the German Foreign Intelligence Service (BND) was inadequate. The oversight body's remit is restricted to BND's technical surveillance against foreigners outside of Germany and BND's cooperation with foreign intelligence services. The oversight body will perform ex ante and ex post oversight and have right of access to all information in BND's system. It will not have a duty to report its findings to the general public. It will, however, report to the **Parliamentary Oversight Panel** of the German Bundestag.

[Link to G10's website here](#)

[Link to the Parliamentary Oversight Panel's website here](#)

[Link to the Independent Control Council's website](#)

[Read more about the German oversight system on the German data protection authority's website](#)

## France

In addition to the parliamentary oversight committee (**DPR**), there is an independent oversight committee, the **CNCTR** (National Oversight Commission for Intelligence-Gathering Techniques), which was established in 2015.

The French oversight body oversees *ex ante* and *ex post* the use of secret surveillance measures in order to ensure that such measures are lawfully carried out within the French territory. Its oversight extends to all public authorities entitled to carry out such measures, including intelligence agencies, police forces and prison administration.

The chair of the commission must be a member of the supreme court for administrative justice (*Conseil d'Etat*) or a member of the supreme court for civil and criminal law (*Cour de cassation*). He or she is appointed by the president of France. The commission consists of four members of the Parliament, two members of the *Conseil d'Etat*, two members of the *Cour de cassation* and one expert in electronic communications.

The CNCTR can request the prime minister to stop certain operations and, if its request is not complied with, the commission can forward the matter to the administrative law court Conseil d'État.

Unlike many other expert oversight bodies, the CNCTR does not have access to information that the French services have obtained from abroad.

The CNCTR also plays a role in overseeing how the intelligence services use algorithms, and it has direct access to some services' systems from its own premises.

[Link to CNCTR's website here](#)

The French data protection authority (National Commission on Informatics and Liberty) also has a limited a role in the oversight of the French services.

## The UK

The UK's oversight of its intelligence and security services has three main components.

There is a parliamentary oversight committee, the **Intelligence and Security Committee of Parliament (ISC)**, whose members are drawn from both Houses of Parliament – the House of Commons and the House of Lords. The Committee oversees the UK intelligence and security services. The scope of its remit is broader than simply reviewing legality; the Committee also oversees policies, expenditure, administration and operations in the services.

[Link to the Committee's website here](#)

There is also a body that conducts both ex ante as well as ex post oversight of all British authorities with investigatory powers, including the British intelligence service. This body is called the **Investigatory Powers Commissioner's Office (IPCO)**.

It is an independent oversight body, but the Commissioner is appointed by the prime minister.

IPCO is an expert oversight body consisting of experienced judicial commissioners with chief responsibility for oversight and prior approval through the double lock system. The double lock systems means that when there is use of certain coercive measures it requires both political approval and approval by IPCO.

This applies, for example, to equipment interference and the collection of bulk data sets.

IPCO has separate units for ex ante oversight and ex post oversight. The ex post oversight is more based on inspections. IPCO also has a Technology Advisory Panel. This is a panel of technology specialists that advise IPCO on technological matters.

IPCO's remit also includes contact with the general public, for example academia and NGOs.

[Link to IPCO's website here](#)

The **Investigatory Powers Tribunal (IPT)** considers complaints against public authorities that are permitted to use investigatory powers, including the intelligence and security services. The IPT has full right of access to information, regardless of whether it is classified. There are however limitations in some cases as regards what can be made known to the complainant about the results of the investigation of a complaint.

The IPT can award compensation to complainants who have suffered an injustice, and make binding decisions to stop ongoing surveillance or demand that information be deleted. The IPT can also consider complaints concerning the refusal of security clearance for members of the UK intelligence and security services.

The IPT is independent of the executive and legislative powers of the UK.

[Link to IPT's website here](#)

The UK also has an [Independent Reviewer of Terrorism Legislation](#).

## The Netherlands

The Netherlands has separate oversight bodies for ex ante and ex post oversight.

The use of certain powers by the intelligence and security services requires the approval of the ex ante oversight body, the Investigatory Powers Commission (**TIB**).

[Link to TIB's website here](#)

The Review Committee on the Intelligence and Security Services (**CTIVD**) is the ex post oversight body. In order to safeguard its independence, the committee members are appointed through a fairly complex procedure that involves all branches of government as well as the Ombudsman, the president of the High Court and the vice-president of the Council of State.

The members of CTIVD are not politicians and work more or less full-time.

CTIVD cannot make binding decisions in investigations it raises on its own initiative. However, its Complaints Handling Department has the mandate to issue binding decisions on the intelligence and security services.

The oversight body has full access to the services and direct access to their systems.

CTIVD has an expert group that it makes active use of in its oversight activities and as a source of general input. The oversight body itself also has an advisory role in relation to legislation.

Its investigations are often thematic. CTIVD publishes a public version of its reports as each investigation is completed. The annual report summarises that year's investigations.

[Link to CTIVD's website here](#)

*The Netherlands also has the Committee for the Intelligence and Security Services (**CIVD**) in the parliament.*



## Belgium

The country's ex ante oversight body is the **SIM Commission** that performs oversight over specific intelligence methods.

Belgium's ex post oversight body is the **Standing Intelligence Agencies Review Committee (Standing Committee I)**.

Standing Committee I has a broad remit that includes reviewing legality as well as overseeing how effective the services are.

The Committee reports to the Belgian Parliament, but its members are experts. Persons employed by the police or intelligence services may not be appointed to the committee.

The oversight body also considers complaints, and an affiliated body considers complaints about security clearance. This affiliated body can make binding decisions.

Both chambers of the Belgian Parliament as well as the government can ask the Committee to investigate certain matters. The oversight body must inform parliament of any oversight activities conducted on its own initiative.

The committee has an advisory role in relation to legislation, and in some cases also in relation to judicial authorities.

[Link to Comite I's website here](#)

## Switzerland

Switzerland has a parliamentary control delegation as well as an external oversight body, the Independent Oversight Authority for Intelligence Activities (**OA-IA**).

In addition to reviewing legality, OA-IA oversees the effectiveness of the Swiss intelligence services.

It is an independent oversight body without a committee model, and it is under the authority of the government in administrative matters.

The oversight body cannot make binding decisions. If a recommendation is not complied with, OA-IA can demand that the Federal Council (equivalent to the government plus the head of state) looks into the matter.

OA-IA is not an appellate body. Complaints against the intelligence services are considered by the Federal Data Protection and Information Commissioner, which also plays a role in the oversight of the Swiss services.

There is also local intelligence oversight at canton level in addition to federal oversight.

[Link to OA-IA's website here](#)

[Link to the control delegation here](#)

*Switzerland also has a separate oversight body that oversees the Swiss intelligence services' use of SIGINT, including intelligence activities targeting cable traffic.*

## The USA

The USA has **two congressional oversight bodies**, both of which are independent bodies made up of serving politicians. The **House Permanent Select Committee on Intelligence** is the House of Representatives' oversight body. It was established in 1977 and oversees all the USA's intelligence services and activities. The Senate counterpart is the **Senate Select Intelligence Committee**, which was established in 1976 and has a similar remit as the committee in the house.

The intelligence services have **Inspectors General (IG)**. They oversee, audit and investigate matters in the services, and are appointed by the president and confirmed by the Senate.

Such inspectors general are found in the CIA (which has had an IG since 1952), the NSA, the Department of Homeland Security etc. There is also an Inspector General of the Intelligence Community. The FBI is subject to the Inspector General of the U.S. Department of Justice.

Inspectors general have a broad remit. In addition to conducting reviews of legality, they also oversee the services' finances and effectiveness, receive complaints from employees/whistle-blowers as well as the public, and can investigate criminal offences in the services.

As a rule, the inspectors general shall have unlimited access to information, although top executives and some ministers can deny access to particularly sensitive material. If access is denied, the congressional oversight committees will be informed.

**The Privacy and Civil Liberties Oversight Board (PCLOB)** was established in 2004 on the recommendation of the 9/11 Commission. The board's members are appointed by the president and confirmed by the Senate. The PCLOB is an independent agency within the Executive Branch; it is not part of the intelligence services.

The PCLOB shall have access to all the information it requires in the performance of its oversight duties. The PCLOB oversees that the public authorities' anti-terrorism measures are balanced against considerations for protection of privacy and civil liberties, and it considers proposed anti-terrorism legislation before it is implemented. Advisory and oversight functions are thus combined in the PCLOB.

**Privacy and Civil Liberties Officers** serve certain departments and agencies, including the Office of the Director of National Intelligence, NSA, CIA, and FBI. These officers have statutory duties relating to the protection of privacy and civil liberties and the receipt and review of complaints.

As of October 2022, President Biden's Executive Order 14086 establishes **the Data Protection Review Court (DPRC)**. It is a body that will handle qualifying complaints, the decisions by the Court's judges are binding on the intelligence agencies.

There is also the **President's Intelligence Advisory Board (PIAB)**, which advises the president on the quality and legality of the USA's foreign intelligence activities.

Finally, there is the **Foreign Intelligence Surveillance Court (FISC)**, which is part of the Judiciary, a wholly independent branch of government. This specialist court rules on applications from the intelligence services for permission to conduct certain

operations/surveillance activities, and it exercises judicial oversight over the execution of those orders. The FISC can direct that the government remedy any compliance problems, and can order the deletion of improperly collected data, as well as the suspension or stopping of relevant surveillance activities.

*Links to the different US oversight bodies:*

- [\*The office for the inspector general of the intelligence community\*](#)
- [\*House Permanent Select Committee on Intelligence\*](#)
- [\*Senate Select Intelligence Committee\*](#)
- [\*The Privacy and Civil Liberties Oversight Board\*](#)
- [\*The Inspector General of the Justice Department\*](#)
- [\*The Inspector general of the NSA\*](#)
- [\*Foreign Intelligence Surveillance Court\*](#)

## Canada

Few countries have a longer tradition of independent oversight of the intelligence and security services than Canada.

The current ex post oversight body is quite new, established in 2019. It is called the **National Security and Intelligence Review Agency (NSIRA)**. NSIRA is supported by a secretariat. The secretariat is anticipated to grow to more than 100 over time. NSIRA was created through the merger of two oversight bodies. The remit of the merged oversight body also includes all national security or intelligence activities that have not previously been subject to such oversight.

NSIRA has a mandate that covers the investigation of complaints against several intelligence and security services, as well as security clearance cases.

One particularly interesting feature of NSIRA is that, in principle, it is the oversight body that ultimately decides, after consultations, what information it chooses to communicate with the general public through annual reports etc. The government nevertheless can bring the matter before a court if they have strong objections. The court will then make a decision in the case.

NSIRA is also mandated to receive information from whistle-blowers.

NSIRA's committee members are experts appointed by the prime minister.

[Link to NSIRA's website here](#)

There is also the **National Security and Intelligence Committee of Parliamentarians (NSICOP)**. This is a committee consisting of serving members of parliament. NSICOP's mandate is mainly to review the legislative, regulatory, policy, administrative and financial framework for national security and intelligence.

[Link to NSICOP's website here](#)

NSIRA and NSICOP are required by law to coordinate their activities to avoid duplication.

The Federal Court of Canada and **the Intelligence Commissioner**, established in 2019, are both ex ante oversight bodies that authorize intelligence operations of the Canadian intelligence services.

[Link to the Intelligence Commissioner's website](#)

## Australia

Australia has a Parliamentary committee, the **Parliamentary Joint Committee on Intelligence and Security (PJCIS)**, and an independent oversight body, the **Inspector-General of Intelligence and Security (IGIS)**.

The Inspector-General is an independent statutory office holder appointed by the Governor-General on recommendation of the government. IGIS reviews the activities of six intelligence agencies for legality, propriety, and consistency with human rights obligations. Recent legislation changes have expanded IGIS' jurisdiction to include specific activities of two additional agencies.

The Inspector-General can also investigate complaints made against the intelligence agencies in its jurisdiction. Complaints can be made by a member of the public, or by a current or former employee of an intelligence agency.

The IGIS engages with the Parliamentary Committee regularly on areas of mutual jurisdiction.

[Link to the Australia Inspector-General's website here](#)

Australia also has an [Independent National Security Legislation Monitor](#).

## New Zealand

The oversight body was established in 1996 – the **Inspector-General of Intelligence and Security (IGIS NZ)**.

The Inspector-General and Deputy are formally appointed by the Governor-General, on the recommendation of the House of Representatives.

IGIS NZ's jurisdiction covers the two intelligence and security agencies, but not intelligence activities carried out by other NZ agencies, for example, by the military.

The Inspector-General has statutory right of access to both intelligence and security agencies' security records. The IGIS can request information or interview people who are in possession of information relevant to an IGIS inquiry. The IGIS can also receive and investigate complaints about the Intelligence and security services. It is a criminal offence to obstruct the work of the Inspector-General.

[Link to the New Zealand Inspector-General's website here](#)

New Zealand also has a parliamentary committee – the **Intelligence and Security Committee**. The Committee considers the annual reports of IGIS NZ and can request the Inspector-General to open investigations.

[Link to the Committee's website here](#)

New Zealand has a body called the **Commissioner of Intelligence Warrants** that does limited ex-ante oversight – its mandate is restricted to intelligence warrants against New Zealand Nationals.

## Norway

The Norwegian Parliamentary Oversight Committee on Intelligence and Security Services (EOS Committee) is a permanent oversight body for “the secret services” in Norway. The Committee is responsible for continuous oversight of the Police Security Service (PST), the Norwegian Intelligence Service (NIS), the National Security Authority (NSM), the Defence Security Department (FSA) and other public authorities that perform intelligence and security services whose purpose is to safeguard national security interests.

The Committee was established in 1996 and is independent of the services and the public administration. The members are elected by the Storting (the parliament), and the Committee reports to the Storting in the form of unclassified annual reports and special reports.

Continuous oversight is carried out by means of regular inspections, both at the services’ central headquarters and at external units. The Committee also handles complaints.

### **Appointment and composition of the Committee**

The seven members are elected by the Storting in a plenary session on the recommendation of the Storting’s Presidium. The Committee conducts its day-to-day work independently of the Storting. Members of the Storting are not permitted to be simultaneously members of the Committee. Persons who have functioned in the services may not be elected to the Committee.

The Storting has emphasized that the Committee should have a broad composition, representing both political experience and experience of other areas of society. Five of the current seven members are elected on basis of their political and professional background. The remaining two are elected on basis of their respective judicial and technological expertise.

### **The area of and the purpose of the oversight**

The purpose of the oversight is primarily to safeguard the security of individuals under the law. It is the Committee’s job to establish whether anyone is being subjected to unjust treatment and to prevent this from occurring, and also to ensure that the EOS services do not make use of more intrusive methods than necessary. The Committee is also required to carry out oversight to ensure that the EOS services conduct their activities within the law.

### **Inspections and about the services**

The Committee inspects the headquarters of the PST, the NSM, the NIS and the FSA several times each year. The services’ external units are also regularly inspected. Normally the services are notified of inspections, but inspections may also be carried out without prior notice.

With one small exception the Committee may demand direct access to the administration’s archives and registers, systems, premises, installations and facilities of all kinds. Anyone that is or has been employed by the services, is obliged to give evidence to the Committee concerning all matters experienced in the course of their duties if summoned.

The main duties of the Police Security Service involve prevention and investigation of illegal intelligence activities, terrorism, proliferation of weapons of mass destruction and export control. The Committee’s inspection of the PST is focused on the service’s handling of personal data, new and closed preventive cases and investigations, the use of covert measures and exchange of information with partners in Norway and abroad.



The NSM's responsibilities are of a preventive nature. The Committee's most important duty in the oversight of NSM is to oversee the service's handling of security clearance cases. The Committee performs oversight of all security clearance authorities within both the defence establishment and the civil service.

The Committee also oversees NSM's other activities, such as the National Cyber Security Centre that handles severe computer attacks against critical infrastructure and information.

The duty of the NIS is to gather, process and analyse information regarding Norwegian security interests in relation to foreign states, organizations or individuals. This means that the activities of the service are directed towards external threats, i.e. threats outside Norway's borders. The NIS is a part of the military, but is both a civil and military intelligence service. It cooperates with corresponding services in other countries. A major responsibility in overseeing the NIS involves ensuring compliance with the prohibition against surveillance of Norwegians on Norwegian territory and requiring that the service is under national control.

The FSA's primary responsibility is the protective security service and operative security of the Armed Forces, including responsibilities related to the Armed Forces' security intelligence. The FSA shall counteract security threats associated with espionage, sabotage, and terrorist acts that may affect military activities and/or national security. The Committee's inspections at the FSA primarily focus on security clearance cases, but the service's responsibilities associated with security intelligence in the Armed Forces also represent a key aspect of the Committee's oversight activities.

## **Complaints**

Anyone who believes that the EOS services may have committed injustices against oneself may complain to the EOS Committee. Complaints are investigated in the service concerned. The investigation is partially done in writing and partially on site by checking archives and registers. Complaints to the Committee are dealt with in confidence, but when a complaint is investigated, the service concerned is informed. If the investigation reveals grounds for criticism, this is indicated in a written statement to the service concerned.

Whistle-blowers also has an opportunity to send information to the Committee. If the whistle-blower wants to remain anonymous, the Committee will do what it can to keep the whistle-blower's anonymity.

The Committee has no authority to instruct the services to take specific action concerning a matter (*this applies to both complaints and other issues*), but may express its opinion, and may make recommendations to the services. The Committee will send an unclassified letter to the complainant stating if there are grounds for criticising the service or not.

## **The Secretariat**

The primary responsibility of the Secretariat is to take care of the daily operations of the Committee. This includes preparation and follow-up of the Committee's internal meetings, inspections and case handling. However, the Committee always makes the decisions in cases and investigations. The Secretariat has year-end 2022 22 employees, and is divided into a legal unit, a technological unit and an administrative unit. The plan is to have 30 employees in the secretariat in 2025.

[Read more on the EOS Committee's website](#)

***The information in this document was up to date as of end 2022 and was written by the secretariat's communications adviser Arild Færaas.***