

Abbreviated annual report 2010

**The Norwegian Parliamentary Intelligence
Oversight Committee
(The EOS Committee)**

PREFACE

The EOS Committee is required by law to submit an annual report on its activities to the Norwegian Parliament, the Storting. This abbreviated annual report for 2010 presents some of the main cases discussed in the comprehensive report. The annual report is available in its entirety in the original Norwegian version at the Committee's web pages, www.eos-utvalget.no.

Chapter 1 describes the mandate and composition of the Committee. Chapter 2 provides an overview of the Committee's oversight of the services, including inspections, investigations of complaints and issues addressed on the Committee's own initiative. Important meetings, conferences and study trips both domestically and internationally are also briefly discussed. Chapter 3 to 6 give an account of the oversight of the Norwegian Police Security Service (PST), the Norwegian National Security Authority (NSM), the Armed Forces' Security Section (FSA) and the Norwegian Intelligence Service (NIS).

In 2010 the Committee focussed on PST. It raised issues related to principles and practice regarding the security service's use of coercive measures and registration of individuals, and raised questions relating to the scope of the Committee's right of inspection of the security service. This has contributed to important clarifications between the Committee and the service.

The security and intelligence services have, in general, demonstrated a good understanding of the Committee's oversight. The experiences from the Committee's activities in 2010 have also shown that the oversight contributes to ensuring the civil liberties of the individual – thus creating trust that the services operate within their legal framework.

Pursuant to the Act relating to the oversight of Intelligence, Surveillance and Security Service, the Committee's reports to the Storting shall be unclassified. According to the Act, the issuer of information shall determine what constitutes classified information. Before a report is submitted to the Storting, the respective sections of the report text shall be submitted to the services in order to ascertain whether or not this requirement has been met. This abbreviated report has been submitted in the same manner.

Content

1.	MANDATE AND COMPOSITION OF THE COMMITTEE	4
1.1	MANDATE OF THE COMMITTEE.....	4
1.2	THE COMPOSITION OF THE COMMITTEE.....	4
2.	OVERVIEW OF THE COMMITTEE'S ACTIVITIES IN 2010.....	5
2.1	THE INSPECTIONS.....	5
2.2	COMPLAINTS AND ISSUES RAISED ON THE COMMITTEE'S OWN INITIATIVE	5
2.3	INVESTIGATIONS OF POLICE METHODS IN THE ARNE TREHOLT CASE.....	5
2.4	MEETINGS, VISITS AND PARTICIPATION AT CONFERENCES	6
3.	THE NORWEGIAN POLICE SECURITY SERVICE (PST).....	6
3.1	INSPECTIONS – AND GENERALLY ABOUT THE OVERSIGHT OF THE SERVICE	7
3.2	THE COMMITTEE'S RIGHT TO ACCESS IN RUNNING OPERATIONS	7
3.3	INSPECTION OF ARCHIVES AND RECORDS	7
3.4	PST'S USE OF COVERT COERCIVE MEASURES	8
3.5	THE NORWEGIAN POLICE SECURITY SERVICE'S PROCEDURE FOR HANDLING REQUESTS FOR DECLASSIFICATIONS AND ACCESS.....	8
3.6	EXCHANGE OF PERSONAL INFORMATION WITH FOREIGN PARTNER SERVICES	9
3.7	COOPERATION BETWEEN THE PST AND THE IMMIGRATION AUTHORITIES.....	10
4.	NORWEGIAN NATIONAL SECURITY AUTHORITY (NSM).....	10
4.1	GENERALLY ABOUT OVERSIGHT OF THE SERVICE.....	10
4.2	QUESTION REGARDING ACCESS INTO A REPORT FOR A SECURITY CLEARANCE INTERVIEW.....	10
4.3	THE COMMITTEE'S OVERSIGHT OF OTHER CLEARANCE AUTHORITIES.....	11
5.	THE ARMED FORCES' SECURITY SECTION (FSA).....	13
5.1	INSPECTIONS AND OVERSIGHT OF THE SECTION.....	13
5.2	THE COMMITTEE'S RIGHT TO ACCESS	14
5.3	CASES FROM THE OPERATIVE SECURITY SECTION.....	14
5.4	CASE PROCESSING OF CLEARANCE CASES.....	15
5.5	COMPLAINANT'S ACCESS INTO CLEARANCE CASES	16
6	THE NORWEGIAN INTELLIGENCE SERVICE (NIS)	16
6.1	GENERALLY ABOUT INSPECTIONS AND OVERSIGHT OF THE SERVICE.....	16
6.2	CASES TO BE SUBMITTED TO THE MINISTRY OF DEFENCE.....	17
6.3	COOPERATION BETWEEN THE INTELLIGENCE SERVICE AND THE NORWEGIAN POLICE SECURITY SERVICE (PST).....	17
6.4	OVERSIGHT OF THE SERVICE'S TECHNICAL ACQUISITION OF INFORMATION.....	17
6.5	EXCHANGE OF INFORMATION WITH FOREIGN COLLABORATIVE SERVICES.....	18

1. MANDATE AND COMPOSITION OF THE COMMITTEE

1.1 Mandate of the Committee

The EOS Committee is responsible for continuous oversight of the intelligence, surveillance and security services (the EOS services) performed by the public authorities, or under management of public authorities. The mandate of the EOS Committee is contained in the Act relating to the Monitoring of Intelligence, Surveillance and Security Services (the EOS Act) – and the Instructions for Monitoring of Intelligence, Surveillance and Security Services. The Act and instructions were last amended in June 2009. The Act relating to Protective Security Services, the Act relating to the Norwegian Intelligence Service and the Instructions for Defence Security Service refer to the Act relating to the Monitoring of Intelligence, Surveillance and Security Services which stipulates that the services are subject to the oversight of the EOS Committee.

The primary task of the Committee is to ensure that intelligence and security services do not violate the civil liberties of the individual. The Committee shall ensure that the services operate within the framework of laws, regulations and non-statutory law. The oversight primarily takes the form of inspections of the archives, computer systems and facilities of the services. The oversight of individual cases and operations is retrospective. But the Committee has full access to information and is constantly updated on ongoing cases.

The Committee must carry out its oversight in a manner that minimises interference with the services' ongoing operations. Special consideration must be given to the need to protect information received from foreign partner services and the protection of sources.

The Committee shall investigate all complaints made by individuals and organisations. Any complaint of, or complaint with reference to, injustices committed by the services will be investigated by the Committee.

1.2 The Composition of the Committee

The EOS Committee has seven members. The members are elected by the Storting in plenary session upon recommendation from the Storting's Presidium. The term of office is normally five years, but members can be re-elected. Members of Parliament cannot serve on the Committee. The Storting has emphasised diversity in the Committee, both in terms of political experience and experience from other areas of society being represented on the Committee. The Committee carries out its tasks independently of the Storting.

The Committee is chaired by *Helga Hernes*, senior advisor at Peace Research Institute Oslo, former state secretary at the Ministry of Foreign Affairs, and ambassador to Austria and Switzerland. Deputy chair of the Committee has been *Svein Grønnern*, secretary general of SOS Children's Villages in Norway and former secretary general of the Norwegian Conservative Party. Other members of the Committee are *Trygve Harvold*, senior advisor and former director of Lovdata; *Gunhild Øyangen*, former Member of Parliament and minister for the Norwegian Labour Party; *Knut Hanselmann*, mayor of Askøy Municipality and former Member of Parliament for the Progress Party; *Theo Koritzinsky*, former professor at Oslo University College, former Member of Parliament and leader of the Socialist Left Party, and *Wenche Elizabeth Arntzen*, district judge on the Oslo District Court and former solicitor.

2. OVERVIEW OF THE COMMITTEE'S ACTIVITIES IN 2010

2.1 The inspections

The EOS Committee's Instructions for Monitoring of Intelligence, Surveillance and Security Services state that the inspections shall at least include the following:

- Six annual inspections of the Norwegian Police Security Service's (PST) headquarters, and at least four local inspections of PST units in different police districts
- Quarterly inspections of the Norwegian National Security Authority (NSM) and of at least two clearance authorities outside the NSM
- Three annual inspections of the Armed Forces' Security Section (FSA)
- Bi-annual inspections of the Norwegian Intelligence Service (NIS) and of at least two external units of the service and/or security and intelligence functions in military staffs and units and of the personal security services of at least two ministries/agencies
- Inspections at the Committee's initiative of the general police force and other bodies or institutions who assist the Norwegian Police Security Service
- As well as other inspections as intended by law

The Committee conducted a total of 28 inspections in 2010, of which 11 were of the services' external branches. The Committee's technical expert participated in seven of the inspections.

An important part of these inspections are the briefings the services provide of their ongoing operations and on issues the Committee requests ahead of the inspections. This provides useful insight into current issues. It also provides a basis for specific questions and for addressing more general and principal issues.

The Committee held 22 internal meetings to prepare and follow up inspections. The Committee has also investigated complaints and addressed issued on its own initiative.

2.2 Complaints and issues raised on the Committee's own initiative

In 2010, the Committee received 21 complaints relating to the EOS services, compared with 19 in 2009. The Committee also received seven complaints that were not directly directed at any of the services. These complaints have been dismissed on formal grounds, with reference to the Committee's oversight being retrospective, that the complaint is not specified or falls outside the Committee's area of oversight. However, the Committee provided guidance to those who filed the complaints as to which body they could address their complaint.

The Committee raised 23 issues on its own initiative in 2010. The most extensive of these was the study on police methods during the Arne Treholt case.

2.3 Investigations of police methods in the Arne Treholt case

Based on public allegations made in the Arne Treholt case, regarding methods used by the former Police Surveillance Agency (POT), the EOS Committee decided in September 2010 to investigate the matter:

"The Committee will investigate whether the Police Surveillance Agency (POT), or any other EOS service, used illegal or irregular methods in the Arne Treholt case. Should this be the case, the Committee will map the extent of such methods, their legality, who knew of the methods used and who authorised them."

Ministers and ministry appointees are not obligated to meet or testify before the Committee. But it will be relevant to ask officials to testify on a voluntary basis. The investigations into this case lead to the Storting allocating additional funds for the Committee and secretariat, and for the use of police and legal expertise. The Committee will present its findings in a special report to the Storting, pursuant to section 13 of the Instructions for Monitoring of Intelligence, Surveillance and Security Services.

2.4 Meetings, visits and participation at conferences

Over the course of the year, members of or the entire Committee have met with various authorities and oversight bodies in Norway and abroad. Members and the secretariat have also participated in several conferences. Some of these are mentioned below in chronological order:

In Norway

The Committee chair held a briefing during a conference for Norwegian *clearance authorities*, organised by the NSM.

- In March, the Committee met with the *Standing Committee on Scrutiny and Constitutional Affairs*. The Committee gave a general briefing on its work and a more specific account of the technical challenges the Committee faces, the services' international collaboration and exchange of information with international oversight bodies.
- In October, members of the Committee met with the *Minister of Justice*. One of the questions discussed during the meeting was individuals' right of access to older information in the PST's archives and records.
- In October 2010, the Committee received a delegation from the *Swedish Government Oversight Committee for the Military Intelligence Service (SIUN)*, established in 2009, which is the oversight Committee for military intelligence services in Sweden.
- In October 2010, a delegation from the Montenegrin parliament visited the Storting. The Committee chair gave an account of the Norwegian oversight arrangement.
- In December, the Committee met with the *Communications Control Oversight Committee (KK-utvalget)* which ensures that the regular police's use of communications control is done in accordance with laws and regulations. It was agreed that the EOS Committee and the Communications Control Committee should meet in the future to share experiences.

Internationally

Some Committee members participated in the International Review Agencies Conference in Sydney, Australia, in March 2010.

- One Committee member gave an account of the Norwegian oversight of the EOS services during a conference for parliamentary oversight bodies in Southeast Europe, held in *Zagreb, Croatia*, in July.
- One Committee member participated at the sixth conference for parliamentary control bodies for intelligence and security services in EU countries in Brussels, Belgium, in September.
- In January 2011, the book "International Intelligence Cooperation and Accountability" was published. The book is financed by the Geneva Centre for the Democratic Control of Armed Forces (DCAF) and the EOS Committee. It is based on the lectures held during the international conference "Accountability of International Intelligence Cooperation", organised by the Committee together with DCAF and the Human Rights Centre at the University of Durham in Oslo in October 2008.

3. THE NORWEGIAN POLICE SECURITY SERVICE (PST)

3.1 Inspections – and generally about the oversight of the service

In 2010, the Committee carried out six inspections of the Central Unit (DSE), as well as inspections of the security service units in the Follo, Haugaland and Sunnhordland, Hordaland and Hedmark police districts.

– In 2010, nine complaints against PST were filed by individuals, compared with 16 complaints in 2009. All complaints not dismissed due to formalities, have been investigated by The Committee. The Committee frequently receives inquiries from persons who have had their applications for access into information in PST's archives and records rejected.

In 2010, the Committee focussed on principles regarding its access to information in PST. PST has in some types of cases suspended the Committee's access without adequate grounds and partly provided insufficient information. In 2010, the Committee also raised questions regarding PST's use of covert coercive measures in some instances.

3.2 The Committee's right to access in running operations

During an inspection of the Central Unit in 2010, the Committee received information about a new investigation and was informed that due to the sensitive nature of the case, the Committee would not be privy to the content before the investigation was completed. The service emphasised that the reason why the case had not been submitted was solely because they wished to prevent dissemination of information.

In a letter, the Committee pointed out that it does have right of access into measures and operations in ongoing investigations. The main point of the oversight being conducted retrospectively is that the Committee shall not instruct the services or be used by the services for guidance, cf. Section 2, final subsection of the Act relating to the Monitoring of Intelligence, Surveillance and Security Services and Section 7, first subsection, of the Instructions for Monitoring of Intelligence, Surveillance and Security Services. The Committee also stated:

"The limitations to the Committee's right to access to the services are stipulated in Section 5 of the Instructions for Monitoring of Intelligence, Surveillance and Security Services, which state that the Committee shall not seek more extensive access into classified information than is necessary for purposes of monitoring, and that the Committee shall, as far as possible, observe consideration for protection of sources and information received from abroad. However, it is up to the Committee to assess the extent of the access the Committee should seek in classified cases, based on the oversight task and oversight purposes."

Based on the above, the Committee requested that the case be submitted under the subsequent inspection of the Central Unit. The service granted the Committee's request. *The Committee assumes that the PST in the future does not exempt a case from the Committee with the same basis as originally given in this case* (Annual report, ch. III.2).

3.3 Inspection of archives and records

During each inspection of the Central Unit, spot checks and searches are carried out of the intelligence register after preparations from the secretariat. The Committee performs close and regular control of PST's processing of personal information about individuals. The control is especially focused on the regulatory requirement of necessity, relevance and quality of the information. The result was that about 40 individuals were deleted from PST's intelligence register in 2010.

Registration due to religious and political convictions, etc.

In 2010 the Committee discovered several instances where PST's processing of information violated Section 15 of the Regulations concerning the Norwegian Police Security Service: "Information about a person cannot be treated solely on the basis of what is known

about the ethnicity or nationality of the person, the person's political, religious or philosophical beliefs, union affiliation or information regarding health or sexual preferences." The Committee asked the service to provide an account of which criteria or factors need to be present for the service to be able to treat information about these aspects. In its reply to the Committee, PST wrote:

"Section 15 of the PST Regulations stipulates that information of the type mentioned in the regulations cannot be the only criteria. As a result, the registration must be in accordance with necessity and an assessment of relevance as stipulated by Section 13 (2), first subsection, litera b and Section 14 of the PST Regulation. To treat information of the type included in Section 15 of the PST Regulations will as such not be incorrect as long as it is in addition to information already available and which makes the subject relevant to PST. ...The intent of a person's will and ability to use violence, as well as the relation the person in question may have to a violent organisation, will have significance in the assessment of whether it is relevant for the PST to process information about the person."

Following this, the service, after a renewed assessment, chose to delete 15 of the registrations the Committee had addressed. Some of these included information regarding religious conviction, while others were on political conviction (Annual report, ch. III.3.2).

The five-year rule

Information in the PST intelligence register must be deleted when the conditions for processing such information are no longer present, cf. the so-called five-year rule. During the debate about last year's annual report, the Standing Committee on Scrutiny and Constitutional Affairs stressed that it is important that previous registrations must be deleted if they have not been updated in the past five years, on the condition that they are no longer necessary. *The oversight of this item has resulted in the deletion of some registered information in 2010 as well (Annual report, ch. III.3.4).*

3.4 PST's use of covert coercive measures

The Norwegian Police Security Service, like the regular police, may submit a request to the court for permission to use covert coercive measures during an investigation, such as communications control, electronic room surveillance and covert searches. In addition, the PST has the authority to request to use covert coercive measures to *prevent* or *avert* criminal acts that fall under PST's jurisdiction.

The Committee carries out continuous oversight of PST's use of covert coercive measures in individual investigations. It is particularly important for the Committee to check whether the PST's requests to the courts are founded on thorough information, whether PST is using the coercive measures in accordance with the court order and that the surveillance measures cease should the preconditions of the court order no longer be present. The extent of the PST's use of covert coercive measures is also of interest to the Committee. *The oversight of the PST's use of covert coercive measures in individual investigations provided basis for criticism of the service in three individual cases in 2010 (Annual Report ch. III.4.1 and III.4.2).*

3.5 The Norwegian Police Security Service's procedure for handling requests for declassifications and access

General

The Committee processes appeals after the PST and the Ministry of Justice and Police have rejected requests for access, including in very old cases regarding immediate family. This issue has been raised in several of the Committee's annual reports and been discussed with both the PST and the Ministry of Justice and Police without final clarification. One appeal to the Committee was in regards to a woman's father who wanted to know if information about her father had been registered during the Second World War. Five years after the issue was raised, neither the complainant nor the Committee have received a specific reason why no

information has been given as to whether information about him had been registered or not. The Committee believes that, as a rule, the PST should grant access into information which is 30 years or older.

The Committee on Scrutiny and Constitutional Affairs in its recommendation to the EOS Committee's 2009 annual report, stated that the issue of right to access should be addressed. But shortly before the Committee gave its recommendation, on 4 March 2010, the Storting adopted the Police Registration Act. It stipulates that there is no right to access to PST's archives and records. It was also established that the Freedom of Information Act does not apply to the service.

Based on this, the issue of access into older information with PST was raised in a meeting between Committee representatives and Minister of Justice Knut Storberget in October 2010. During the meeting, it emerged that the Ministry was assessing the question of access into older information. This was a follow-up of a number of inquiries from the EOS Committee and comments from the Standing Committee on Scrutiny and Constitutional Affairs to the latest annual report from the Committee.

The Committee's argument

The EOS Committee gave a written account of its views on the issue of access to older information in a letter 23 November 2010, to the Ministry of Justice and Police. The Committee wrote:

"It is the distinct impression of the Committee, based on experience with oversight activities of PST, that neither PST's operations in themselves, nor the collaboration with foreign partner services have been negatively impacted as a result of the oversight under the temporary oversight arrangement...

The Committee is aware that the PST will have the authority to reject all requests once Section 66 of the Police Registration Act enters into force, at the same time as it establishes that the Freedom of Information Act does not apply to the service. It is the view of the Committee that this change in the law, which will effectively cut off access into the service, makes it particularly important that the Ministry assesses whether the right to access into older information should be established by law. The Committee would like to stress that the main rule on classified information being declassified after 30 years still applies to the PST, even after the Police Registration Act enters into force. Unless the Ministry believes it is natural that access requests for all types of information can be rejected, regardless of whether the information is classified or not, and regardless of how old the information is, it would be necessary with a statutory provision....

Another consideration that speaks in favour of a legislated right to access into older information in the PST is the trust the service enjoys. There is reason to believe that a right to access, although limited to older information, could contribute to increasing the trust the general public has in the service. This will also be in line with the general opening of the service in recent years with an active information strategy and use of social media to communicate with individuals."

The Committee will continue to keep itself updated on the Ministry's assessment of access to older information. In 2011, the Committee will also focus on issues related to declassification and access into information that the PST is treating (Annual Report, ch. III.5.3).

3.6 Exchange of personal information with foreign partner services

The Committee's oversight of PST's exchange of personal information with foreign collaborative services in 2010, uncovered one instance where the PST acted in violation of the guidelines. A foreign security service made an identity request to the PST, which informed the foreign security service that the man was unknown to them, but had a previous charge of battery against his wife filed by the ordinary Norwegian police. The identity request was made as the man had been detained by the country's security services.

When asked by the Committee, the service stated that, in accordance with Section 13, second subsection, number 3, the service has the authority to process personal information if it is necessary for the cooperation with the police authorities in other countries. However, following a new review, the PST concluded that “some of the information exchanged can not be deemed relevant in relation to the request made from an [international] service, and that, as such, the information was not exchanged “in accordance with the applicable routine for exchange of information” (Annual Report, ch. III.6). The service decided to delete all registered information regarding this person.

3.7 Cooperation between the PST and the immigration authorities

The cooperation between the PST and the immigration authorities is fairly extensive. This includes exchange of information in immigration cases, including visa, asylum and deportation cases. The Committee has put special emphasis on knowledge about the cooperation between the EOS services and other public authorities in recent years. As the oversight area of the Committee is limited by function, the Committee may also have a more direct oversight responsibility of authorities that cooperate and exchange information with the EOS services.

In the 2009 annual report, the Committee expressed its satisfaction that the guidelines for the cooperation between the immigration services and the PST had been established. In 2010, the Committee has followed this up, by checking that the PST acts in accordance with the regulations stipulated in the new guidelines. In 2010, the Committee inspected the Norwegian Directorate of Immigration (UDI), and received a briefing on the directorate’s cooperation with the PST. *Spot checks of correspondence between the service and the directorate were performed both at UDI and the PST. This gave no grounds for retrospective follow-up* (Annual Report ch. III.7).

4. NORWEGIAN NATIONAL SECURITY AUTHORITY (NSM)

4.1 Generally about oversight of the service

In 2010, the Committee carried out four inspections of the NSM, including one inspection of the NorCERT division, Norway’s national centre for handling computer attacks on infrastructure and information vital to society. The inspection revealed that the division is aware of privacy-related issues. The Committee did not find grounds for further follow-up of individual cases in the division. Furthermore, the Committee inspected the personnel clearance service in the Ministry of Defence and the Norwegian Police Directorate. These inspections did not reveal any grounds for further follow-up.

The Committee received three complaints in relation to security clearances in 2010, the same number as in 2009. One of the complaints was rejected, and one is still being processed by the Committee. The last complaint was in relation to the case processing time for security clearance in the Ministry of Defence. In its completion of the case, the Committee expressed slight criticism in a letter to the Ministry.

4.2 Question regarding access into a report for a security clearance interview

In May 2008, the Committee received an account of how the NSM carries out and reports security clearance interviews. The Committee found principal reasons to address the rights of the interviewee to access into the report from the interview, before a clearance decision was made. In its conclusive letter to the NSM, the Committee expressed the view that in considerations of contradiction and factual information the interviewee should have a right to

access. In comparison, reference was made to the main rule for individual decisions in the government administration giving the party right to access during the case processing. In connection with its debate on last year's annual report, the Standing Committee on Scrutiny and Constitutional Affairs asked to be kept informed about the matter.

In a letter dated 18 January 2010, the Committee asked the NSM to raise the question with the Ministry of Defence whether there exists a need for a change in the access right as stipulated by Section 25a of the Security Act. In a letter dated 2 December 2010, the NSM reported that the service had a meeting with the Ministry to discuss the issue. NSM reported that it might consider assessing rule changes in connection with a general review of the Security Act and regulations in 2011. *The Committee will be informed about further developments and any rule changes in the area.* (Annual Report, ch. IV.3).

4.3 The Committee's oversight of other clearance authorities

Follow-up after inspection of the Norwegian Defence Research Establishment (FFI)

In September 2009, the Committee inspected the personnel clearance service at FFI. Following the inspection, the Committee asked whether certain requirements had been met in a clearance case, i.e. the requirement for basis and the requirement for preparing a report from the security interview. When the case was concluded, the Committee stated that the basis for the decision must be provided together with the notification of the outcome of the clearance case. The FFI had not provided such basis together with the notification because they had made use of an outdated guideline from the NSM, which had been in use before the requirement for concurrent reasons was included in the Security Act in 2006. *The Committee made it clear to the FFI that it must be expected that clearance authorities make sure that security clearance decisions are made on the basis of applicable rules and guidelines.*

During an inspection of the NSM on 8 December 2009, the Committee reviewed dismissed clearance cases decided by the FFI. The cases had been dismissed because the personnel clearance had discovered that they had a criminal record. This information had not been provided in the personal information forms. The Committee had questions regarding FFI's case handling in several of the dismissed clearance cases. FFI said in its reply that the persons in question had failed to provide concrete information and none of the persons would be employed by the FFI. None of the disputed persons had been informed about the dismissal by the FFI, and no written reason had been given.

In the conclusion of the matter, the Committee stressed that the Security Act assumes that a request for clearance usually ends in either a negative or positive *clearance decision*. The Committee stated further that:

"FFI's rejection of clearance cases without formal grounds meant that the persons involved were not granted their right of knowing the reason. Nor did they have any right of notification, access or appeal as stipulated in Sections 25, 25 litera a and 25 litera c of the Security Act. These are, together with the establishment of an observation period, important guarantees for legal safeguards in the case of negative clearance decisions... FFI's handling of these cases shows a number of shortcomings, and involves clear violations of the Security Act's requirements for handling security clearance cases. The fact that there are no written grounds for the dismissal decisions is also censurable. In general, the notoriety of FFI's case handling is unsatisfactory."

The Committee has notified the NSM of the matter. The service has informed the Committee that the issues raised "involved unacceptable practice". NSM will follow up and provide FFI with the necessary guidance in the form of advice, training and preparation of suitable routines (Annual Report, ch. IV.5.1).

Case from the Ministry of Justice and the Police

In the 2009 annual report, the Committee reported that it had asked the Ministry of Justice and Police to carry out a new assessment of an unappealed negative clearance case. The case concerned a person who had been granted the clearance “confidential”, but the requirement was that the clearance only applied to that position. The person was affiliated with another state. But it was not apparent from the decision what considerations the Ministry had made of the affiliation with the state in question, nor which issues had been given emphasis when setting the requirement. Following a new review of the case, the Ministry reported that the previous decision was upheld. In the case documents it emerged that the person had dual citizenship, which had been unknown to the Committee.

Based on the decision of the Ministry it seems that decisive emphasis had been placed on the relationship between Norway and the state in question. In its concluding letter, the Committee stated that it was difficult to see how such general circumstances could solely decide the person’s security qualification. *The Committee concluded that the Ministry of Justice and Police had not treated the case in accordance with the applicable rules. It is assumed that the Ministry in future cases will make specific and individual assessments of possible affiliations that a person may have to other states.* (Annual Report, ch. IV.5.2)

Complaint regarding case processing in a clearance case in the Ministry of Defence

The Committee received a complaint regarding the Ministry of Defence spending two years and four months reaching a conclusion in a clearance case, without the person in question receiving any reply or notification of delays. In its reply, the Ministry admitted that it had spent too much time on the case, and wrote:

“This case is, in our view, not very complicated, and thus, a decisions should have been reached at an earlier stage. Challenges in connection with resources, as well as a change of case officer in the cases where [X] is the requesting authority, have unfortunately resulted in a disproportionately long period of time before a decision was made in this case. This is unfortunate.”

The Committee made the following comments to the long case processing time:

“The Ministry of Defence spent a total of two years and four months making a decision in this case. This is not an acceptable case processing time for security clearance cases, particularly not in this instance, which was not complicated. Based on this, the Committee is pleased that the Ministry of Defence admits that the case processing time was too long, and that the Ministry has apologised ... Long processing times in clearance cases has a direct impact on individuals who risk losing job offers or are prevented from carrying out tasks. A disproportionately long case processing time could therefore weaken legal safeguards for individuals and the trust in the administration. The Committee assumes that this case is not indicative of the practice of the Ministry of Defence in clearance issues.”

In response to the Committee’s question regarding a preliminary reply to the complainant, the Ministry of Defence responded: “The NSM Handbook from 2003 regarding processing of clearance cases did not require a preliminary reply if the processing time was disproportionately long.” The Committee then made the Ministry aware of the fact that the mentioned handbook was outdated as it had not been amended or updated since the changes to the Security Act of 2006 (Annual Report ch. IV.5.4). In its concluding letter, the Committee wrote:

“Over the course of the two years and four months, the Ministry of Defence received a number of written reminders from [the requesting authority] regarding the case. The Ministry must therefore, on a number of occasions, have been aware of the need for a clarification in the clearance case. The Committee assumes that the Ministry of Defence will keep the person in question informed in writing in the future should a case take significantly longer to process than initially stated.”

Inspection of the personnel clearance service in the Ministry of Foreign Affairs

Following the inspection of the personnel clearance service in the Ministry of Foreign Affairs in 2007, the Committee commented on the Ministry's routines for authorising own employees. This issue has been addressed in the three previous annual reports. The Standing Committee on Scrutiny and Constitutional Affairs asked, in connection with last year's annual report, to be informed about clarifications and changes to case processing routines and so forth.

In April 2010, the Ministry of Foreign Affairs reported that new internal routines for the authorisation of ministry employees had been adopted ensuring that the Ministry is in compliance with the requirements stipulated in the Security Act and the Personnel Security Clearance Regulations. A copy of the routines as well as an internal memo regarding the implementation of these was submitted to the Committee. The Ministry also reported that courses will be held for ministry supervisors in conducting clearance interviews. In December 2010, the Committee received further updates on the status of the Ministry of Foreign Affairs' follow-up of this, including information regarding the implementation of clearance interviews which the Ministry has prepared in consultation with NSM.

The Committee has noted that the Ministry of Foreign Affairs is now in compliance with the requirements for authorisation stipulated in the Security Act and the Personnel Clearance Regulations (Annual Report, ch. IV.5.5).

5. THE ARMED FORCES' SECURITY SECTION (FSA)

5.1 Inspections and oversight of the section

In 2010, the Committee carried out three inspections of the FSA, which have given accounts of personnel security, operative issues and work related to information security. In addition, the Committee, during each inspection, reviewed all non-appealed negative clearance decisions made by the FSA since the previous inspection. Based on this, the Committee submitted written questions to the FSA regarding its case processing in several clearance cases in 2010.

The Committee also inspected the section's archives, journals and electronic systems, including individual cases in the Operative Security Section. Furthermore, the Committee raised some legal questions with the FSA regarding the section's military counter-intelligence.

In 2010, the Committee received one complaint from an individual who targeted the FSA, which was also directed towards the PST, NSM and NIS. The complaint was finalised without any criticism. In comparison, the Committee received three complaints against the FSA in 2009.

In last year's annual report, the Committee gave an account of several unanswered issues when the report was submitted to the Storting. During the Storting's debate of the annual report in 2009, the Standing Committee on Scrutiny and Constitutional Affairs emphasised the importance of the EOS services replying to requests from the Committee without undue delays. The issues which were unanswered in 2009 had been answered in 2010, and are in part described below. *The Committee's requests to the FSA in 2010 have been answered as assumed. The Committee is now pleased with the understanding the section has demonstrated of the oversight activity this year.*

5.2 The Committee's right to access

In the 2009 annual report, the Committee reported that the FSA was sceptical to submitting routine memos in its personnel security section to the Committee. In a letter to the Committee in March 2010, the FSA wrote that the service was working on a review of all routine memos, all of which had to be approved and signed by the head of the FSA. The FSA also stated that it had been decided to implement a practice of annual re-signing of all routine memos. FSA continued:

"FOST wishes to confirm that we will keep the EOS Committee informed about changes to the content which will be decided for our routine memos. For practical reasons, FOST suggest that this is done primarily in connection with the Committee's inspections of FOST, where each changed memo will be presented and submitted. In cases of major changes being carried out and initiated quickly, and there is some time until the next inspection, FOST will make sure that the Committee is informed of this. FOST asks that the Committee confirms whether this is a satisfactory arrangement."

Revised routine memos, approved by the head of the FSA, were submitted shortly thereafter. In a concluding letter to the FSA in April 2010, the Committee upheld its request to have the memos submitted each time changes to the content are made, regardless of when the change was made:

"The Committee's oversight of FOST's implementation of the personnel security service is made not solely by the Committee's physical inspections of the personnel security section. It will be useful to be familiar with any changes to routine memos and the application of the regulatory framework in connection with the Committee's preparation for inspections of the services and in general in connection with the Committee's assessment of clearance decisions made by FOST."

The Committee then made an additional request to the FSA to submit changed routine memos for the personnel security service. In a later letter, the FSA confirmed that this practice would be adopted. (Annual Report, ch. V.2)

5.3 Cases from the Operative Security Section

During an inspection of the FSA in April 2009, the Committee reviewed operations carried out by the Operative Security Section. Following the inspection, the Committee had questions regarding some of the FSA's operations. These had been carried out as military counter-intelligence operations. The background for the Committee's questions was in particular that it seemed as though the FSA had carried out planned and covert operations not exclusively directed against military personnel in military areas. The operations included partly observation and photographing civilians in public. The Committee asked whether the FSA personnel had operated covertly or not, and for the legal basis for these operations. At the same time, the Committee also submitted questions both to the FSA and PST regarding their cooperation in these operations.

The FSA acknowledged that the Section "does not have legal authority to carry out systematic observation of private individuals in public", and pointed out that the difference between systematic observation and carrying out general observation assignments, which the Section claimed was authorised under the general freedom of action, was not always easy to draw. The FSA made further note that the general freedom of action gives the FSA the authority to carry out "observational actions" with military counter-intelligence objectives in civilian areas, and characterised this as regular "observation" or "vigilance".

In its concluding letter to the FSA, the Committee noted that it explicitly appeared in some operational orders and operations reports that FSA personnel had in part acted covertly, in contrast to what the FSA had reported to the Committee. In one of the FSA's military counter-intelligence operations, the Committee pointed out that the sections' observations of some persons in public spaces eventually appeared as persistent and personal, bordering on

surveillance. The FSA must be regarded as covertly obtaining information about civilian persons by noting names for follow-up with the PST. The Committee pointed out that the intensity of the FSA's observational actions must be regarded as fairly high. The Committee wrote that the FSA is not authorised to carry out this form of observational operations, nor covertly obtain information about civilian persons outside military areas.

The Committee also noted that FSA personnel had photographed private persons in public spaces using handheld cameras, while posing as civilian guests in the area. The photographs had been collected for military counter-intelligence purposes, in the section's journal system. The Committee pointed out to the FSA that *even* obtaining information using *legal* observation techniques could constitute a disproportionate invasion of privacy. The Committee made reference to a precedent from the European Human Rights Court which has determined that it may be a violation of the prohibition of Section 8 of the European Human Rights Convention against invasion of privacy should subsequent processing of personal information in connection with a certain person enable the information to be retrieved for later use.

Following this, the Committee made it clear to the FSA and PST that it assumes that future cooperation will take place in accordance with the regulatory framework, that there is sound notoriety in the cooperation and that support is given within the framework of own authority. The Committee asked the FSA to carry out an impending review of the personal information which was processed in the operations in questions. The FSA was specifically asked to assess whether it is necessary to store the information, or if it could be deleted. The Committee will follow up the case in 2011. (Annual Report, ch. V.3)

5.4 Case processing of clearance cases

Use of telephone interviews in cases regarding financial issues

In the 2009 annual report, the Committee gave an account of the FSA's use of telephone interviews in clearance cases regarding financial issues. As stipulated in Section 21, third subsection, third item, of the Security Act, a clearance interview shall be held as long as it is not "clearly unnecessary". The Committee commented that financial issues are often complex, which indicates that the person should be allowed to present his/her case in a clearance interview. Following this, the Committee asked the FSA to review its routines for use of clearance interviews.

In 2010, the FSA reported that the section's use of telephone interviews as a substitute for personal clearance interviews had ceased in December 2008. Based on this, the Committee, in its concluding letter to the FSA, stated that it is pleased that the FSA's "by-passing of the requirement to carry out clearance interviews" and "use of telephone conversations in financial issues had ceased". (Annual Report, ch. V.5.1)

Cases regarding the use of narcotics

Based on the review of unappealed negative clearance decisions by the FSA, the Committee had some questions regarding the section's assessment of the use of narcotics. In its oversight, the Committee had observed that the section practised the following routine: Persons who provided information regarding the use of narcotics on the personal information form, but where it did not appear from queries in the registries that the person had any association with narcotics, were asked to give a written account of the issue. In cases where persons failed to provide further information, FSA made negative decisions. The grounds given were that it was impossible to give a satisfactory account of the person's dealings with narcotics. In all cases, it was considered "clearly unnecessary" to carry out clearance interviews.

Based on the section's replies to the questions raised, the Committee commented:

"In its reply to the Committee, FOST writes that the practice of omitting substantive discussions when the person in question has not provided supplementary information in regards to the relevant points on the personal information form, has ceased. The Committee is pleased with this. FOST then continues to write in its reply that when necessary for the assessment of each individual case, the section will continue to request further information, but that the number of clearance interviews in these types of cases will be increased. In this regard, the Committee would like to emphasise that clearance interviews shall be held, except for when this is regarded as "clearly unnecessary", cf Section 21, third subsection, third item, of the Security Act... On this basis, it is assumed that obtaining written additional information in cases of doubt should be used as a supplement, and not as a substitute, for clearance interviews."

The Committee also commented that the section put greater emphasis on individual narcotics cases than other clearance authorities, which the FSA in main agreed with. The section's description of routines was, based on this, amended so that greater emphasis was placed on how long ago the use of for instance cannabis had taken place. The FSA also expressed that they would make specific and individual comprehensive assessments in cases where the use of narcotics is more recent. The Committee finds this satisfactory. (Annual Report, ch. V.5.3).

5.5 Complainant's access into clearance cases

In last year's annual report, the Committee gave an account of a request to the FSA to declassify the correspondence between the Committee and the FSA in connection with the Committee's handling of a complaint.

In the case, the Committee made reference to the stipulation in Section 25, litera a, of the Security Act regarding that the right to access into "the case documents" must also apply to the clearance case in question. During the Storting's debate on last year's report, the Standing Committee on Scrutiny and Constitutional Affairs commented that the documents must be regarded as part of "the case documents", and therefore, access can be requested "on the same conditions as for the other case documents".

The FSA reviewed the question again in 2010, and has informed the Committee that the correspondence has been declassified and that the complainant has been granted access in accordance with Section 25, litera a. In its concluding letter to the FSA, the Committee commented: "giving individuals the right to access into issues regarding their own clearance case and as such, being able to defend their own interests, represents an important legal safeguard". (Annual Report, ch. V.6)

6 THE NORWEGIAN INTELLIGENCE SERVICE (NIS)

6.1 Generally about inspections and oversight of the service

In 2010, the Committee also carried out three inspections of the Intelligence Service centrally. In addition, an inspection was carried out of the service's technical collection activity at the Armed Forces' Testing Station Vadsø and the Armed Forces' Station Vardø. During the inspections, the Committee had special focus on compliance with the prohibition on obtaining information about Norwegian citizens.

The Intelligence Service's systems for technical acquisition of information are being updated continuously, which is demanding from an oversight perspective. In order to meet this challenge, the Committee has followed up the inspection routines established in 2009: The Committee chair, together with the secretariat and technical expert, prepares all inspections.

It is the Committee's experience that this, in accordance with the intention, contributes to a more targeted oversight of the Intelligence Service.

In 2010, the Committee received one complaint against the Intelligence Service, which was also directed at the PST and FSA. The complaint has been concluded without any criticism. In comparison, the Committee received five complaints against the Intelligence Service in 2009.

6.2 Cases to be submitted to the Ministry of Defence

In accordance with Section 13 of the Instructions for the Norwegian Intelligence Service, matters of "particular importance or that raise questions of principle" must be submitted to the Ministry of Defence. For many years, the Committee has had particular focus on sound routines for notoriety and documentation of the political authorisation process. Only then is it possible in retrospect to be familiar with the methods and operations of the service which are submitted to the Ministry.

For inspection at the service's headquarters, the Committee is presented with cases that have been submitted to the Ministry. In 2010, the Committee has looked into several cases in more detail. *It is the impression of the Committee that there now appears to be good notoriety in the cases the service submits to the Ministry, including any legal considerations. The Ministry's assessments are also documented in writing. The Ministry assumes that its authorisation is submitted to the EOS Committee. The Committee is pleased with the awareness which both the Ministry and service now demonstrate in this area. (Annual Report, ch. VI.1).*

6.3 Cooperation between the Intelligence Service and the Norwegian Police Security Service (PST)

In its oversight, the Committee focuses on ensuring that the cooperation between the services is within the legal framework and instructions that apply to each of the services. In 2010, the Committee has been kept informed about the interaction between the PST and the Intelligence Service. The services work continuously to improve the routines for cooperation. In 2010, this resulted in a plan for cooperation, which was presented to the Committee by both services: Firstly, the services will identify legal impediments for the cooperation and prepare routines for cooperation. Furthermore, the services will identify information needs and opportunities as well as limitations on information exchange. They will also consider establishing a liaison arrangement. Furthermore, they will look into the possibility of increasing and exchanging expertise.

During the inspections of PST and the Intelligence Service, the Committee checks specific cases of cooperation, including the exchange of information between the two services, both through briefings from the services and by inspecting archives and registers.

The Committee sees that such cooperation is important for the services, and that people moving across national borders can be problematic as regards to delineating the areas of the PST and Intelligence Service. *The Committee sees it as positive that the services are aware of the challenges the various authorities of the services cause in connection with operational cooperation. The Committee will in 2011 continue to focus on the cooperation between the PST and the Intelligence Service.*

6.4 Oversight of the service's technical acquisition of information

Pursuant to Section 4 of the Act relating to the Norwegian Intelligence Service, the Intelligence Service may not carry out surveillance, or in any other way, covertly obtain information about Norwegian citizens on Norwegian territory. Ensuring that this provision is

not violated constitutes the most important part of the Committee's oversight of the service's technical acquisition of information: This must be carried out in such a manner that it can be stopped if the persons in question are identified as Norwegian citizens.

In one specific case, the Committee raised questions regarding the service's acquisition of information concerning an expatriated Norwegian citizen. The Intelligence Service's reply demonstrated that the service is aware of the regulatory limitations on surveillance of Norwegian citizens on Norwegian territory. The Committee did not find reasons to follow up the case further. *In 2010, the Committee did not discover any cases which violated the prohibition on obtaining information concerning Norwegian citizens, nor did the Committee identify any other nonconformities in connection with the oversight of the technical acquisition of information in the Intelligence Service (Annual Report, ch. VI.3).*

6.5 Exchange of information with foreign partner services

The Committee regularly checks the Intelligence Service's exchange of information with foreign partner services. The service's communication system for exchange of information is used to send and respond to requests mainly related to counterterrorism, which the service is legally obligated to obtain. In this regard, the service depends on cooperation with foreign intelligence and security services. In this cooperation, information is exchanged which supports international operations where Norwegian forces also participate.

The Committee is to check that the Intelligence Service complies with the prohibition in Section 4 of the Act relating to the Norwegian Intelligence Service against the service monitoring or in any other way covertly obtaining information about Norwegian legal subjects. When the Intelligence Service receives information regarding Norwegian citizens from foreign services, this information must either be deleted or forwarded to the PST.

The Committee checks that there is notoriety surrounding the exchange of information, and how foreign requests about Norwegian citizens are received and handled. The control has mainly been carried out as spot checks and searches among dispatches the service has sent abroad.

In the 2009 annual report the Committee gave an account of the Intelligence Service's establishment of a control system to unveil violations of internal routines for the exchange of information. In 2010, the service reported that it had tightened control routines and approval routines for information exchange with partnered foreign services. The service has furthermore stated that courses will be held to strengthen the service's internal routines for this information exchange. *Over the course of the year, the Committee has not received information about, nor in any other way, identified any violations of the internal control routines for information exchange with foreign services, or other regulatory requirements relating to this. (Annual Report, ch. VI.4).*