Abbreviated Annual Report for 2009

Norwegian Parliamentary Intelligence Oversight Committee (the EOS Committee)

PREFACE

Each year, the EOS Committee submits a report to the Norwegian Parliament (the Storting) outlining its activities. This abbreviated annual report for 2009 presents some of the principal issues from the more comprehensive report. References to the full report are provided for important issues. The full annual report is available on the Committee's web pages, www.eos-utvalget.no.

Chapter I provides a brief introduction to the Committee's mandate and composition. Chapter 2 contains an outline of the Committee's oversight activities, including inspections, investigation of complaints and matters raised on the Committee's own initiative. The chapter also provides a brief overview of important meetings, conferences and study visits in Norway and abroad. Chapters 3 – 6 describe the oversight of the Norwegian Police Security Service (PST), the National Security Authority (NSM), the Norwegian Defence Security Service (FOST) and the Norwegian Intelligence Service (E-tjenesten).

With a few principal exceptions, the services' contact with the Committee in connection with oversight activities has been constructive. Experiences from 2009 have shown that the Committee's activities contribute to safeguarding the rights of the individual, as well as generating confidence in the general public 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.

CONTENTS

1. THE COMMITTEE'S MANDATE AND COMPOSITION

1.1 The Committee's mandate

The EOS Committee is responsible for continuous oversight of the intelligence, surveillance and security service (EOS service) performed by the public authorities, or under management of or on commission from the public authorities. The EOS Committee's mandate is contained in the Act relating to the Oversight of Intelligence, Surveillance and Security Service (the EOS Act) and in the Instructions for Oversight of Intelligence Surveillance and Security Service. The EOS Act and Instructions were last amended in June 2009. The Act relating to Protective Security Service and the Act relating to the Norwegian Intelligence Service refer to the EOS Act which stipulates that the services shall be subject to the Committee's oversight. (Annual Report, Chapters I.1 and VIII. 2 and 3).

The Committee's most important task is to prevent injustice against any person during the practice of intelligence, surveillance and security service. Furthermore, the Committee shall ensure that the services work within the framework of statute law, government directives and non-statutory law. The oversight activities are conducted through inspections of the services' archives, computer-based systems and installations. The oversight of individual cases and operations shall abide by the principle of subsequent oversight. It should be arranged in such a way as to interfere as little as possible with the day-to-day activities of the services. The Committee shall observe consideration for protection of information received from cooperating services abroad.

The Committee shall examine all complaints from individuals and organisations. Any complaint or request where a person or organisation claims to be subjected to unjust treatment shall be investigated in the services against which they are directed.

1.2 Composition of the Committee

The EOS Committee has seven members. The members are elected by the Storting in a plenary session on the recommendation of the Storting's Presidium. Deputies are not elected. The term of office is normally five years, but the members may be re-elected. Members of the Storting are not permitted to simultaneously be members of the Committee. The Storting has emphasised that the Committee should have a broad composition, representing both political experience and experience of other areas of society. The Committee conducts its day-to-day work independently of the Storting.

In 2009, the Committee was chaired by *Helga Hernes,* Senior Adviser at the International Peace Research Institute (PRIO), and former state secretary at the Ministry of Foreign Affairs and ambassador to Vienna and Bern. Deputy Chair was *Svein Grønnern*, Secretary General of SOS Children's Villages in Norway and former Secretary General of the Norwegian Conservative Party. The other Committee members were: *Kjersti Graver*, Judge at Borgarting Court of Appeals and former Consumer Ombudsman, *Trygve Harvold*, Managing Director of the Norwegian Legal Database Foundation Lovdata, *Gunhild Øyangen*, former member of the Storting and Council of State for the Norwegian Labour Party, *Knut Hanselmann*, mayor of Askøy Municipality and former member of the Storting for the Norwegian Progress Party and *Theo Koritzinsky*, Associate Professor at Oslo University College, Faculty of Education and International Studies, former member of the Storting and Chairman of the Socialist Left Party of Norway and *Wenche Elizabeth Arntzen*, District Court Judge, Oslo District Court and former lawyer.

2. OUTLINE OF COMMITTEE ACTIVITIES IN 2009

2.1 The inspection activities

Pursuant to the EOS Instructions, the Committee's inspection activities must, as a minimum, include:

- six inspections every year at the Police Security Service's headquarters (PST) and at least four local inspections of PST units in various police districts
- quarterly inspections of the National Security Authority (NSM) and at least two security clearance authorities outside NSM
- three inspections annually of the Norwegian Defence Security Service (FOST)
- semi-annual inspections at the Norwegian Intelligence Service's headquarters (E-tjenesten) and at least two external units of the service and/or security and intelligence functions of military staff or units.

Based on this, the Committee conducted 27 inspections in 2009, 11 of which were of external units. The Committee's technical expert participated in seven of the inspections.

An important part of the inspections is the services' briefings relating to the continuous activities and their account of topics requested by the Committee prior to the inspection. This provides useful insight into relevant topics covered by the services. Moreover, it provides a basis for raising specific questions and more general and fundamental issues.

During the year, the Committee has organised 14 internal committee meetings to, inter alia, plan and follow up on inspections. In addition, the Committee investigated complaints and matters raised on its own initiative.

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

The Committee received 19 complaints relating to the EOS services in 2009. In addition, the Committee received eight complaints not directly related to any of the services. The complaints were rejected on a formal basis with reference to the Committee's oversight activities having to be performed subsequently, or because the complaints related to matters that were outside the Committee's area of oversight. However, the Committee provided guidance as to whom the complaining person or organisation should contact.

In 2009, the Committee investigated 20 matters on its own initiative relating to, for instance, registration of personal data by the PST, the handling of security clearance matters and the Committee's right of inspection.

2.3 Meetings, visits and participation at conferences

In the course of the year, the Committee or parts of the Committee have held meetings with various authorities and control bodies in Norway and abroad. In addition, Committee members and the Secretariat have participated at several conferences. Some of these were:

National

In June*, a meeting was held with the Minister of Defence*. The purpose of the meeting was to inform the Minister of the Committee's inspections of the Norwegian Defence Security Service (FOST). At *a meeting with the Civil Aviation Authority in Bodø*, the Committee received information about access control relating to inspections, regulatory developments

and the interface vis-à-vis the EOS services' inspection work on safety in the Norwegian Airspace. In October, the EOS Committee *organised a seminar on the inspection of concealed coercive measures, etc.* The seminar included a lecture on the Swedish bill relating to signal surveillance (the FRA Act), the Method Control Committee's review of the use and inspection of concealed coercive measures and the tasks and mandate of the Communications Surveillance Oversight Committee. The chair of the Committee participated *at the human rights seminar organised by the Parliamentary Ombudsman for Public Administration* in November.

International
On *a study trip to Berlin in May*, the Committee was informed about the parliamentary control scheme with the German EOS services. The Committee members also met, among others, the German government director-general for the federal intelligence services, a representative of the German ombudsman for personal data protection and the Director of the German foreign intelligence service. Committee members also attended *the fifth conference for the European parliamentary oversight bodies for intelligence and security services* in Tallinn in May. In October, the Chair of the Committee and the Acting Head of the Secretariat attended a conference in England on terrorism, safety and human rights.

3. THE NORWEGIAN POLICE SECURITY SERVICE (PST)

3.1 Inspections – general information about the supervision of the service

In 2009, the Committee carried out six inspections of the Central Unit (DSE). In addition, inspections were conducted of the PST units in the police districts of Romerike, Telemark and Troms, as well as of the Governor of Svalbard's PST functions.

The Committee received 16 complaints directed at the PST from individuals in 2009, compared to 13 complaints in 2008. All complaints were investigated centrally in DSE, as well as in local units when the Committee found reason to do so. Five of the complaints were also directed at one or more of the other EOS services.

The Committee has again raised the issue with the Ministry of Justice and the Police of whether access may be gained to information that is several decades old. Furthermore, the Committee has followed up the issue relating to what extent the PST should, according to the regulations, declassify information which relates to people who have not been registered in the service's files and registers.

3.2 Inspection of archives and registers: Registration and deletion

The Committee checks that the PST only processes information which is necessary and relevant to the performance of its tasks, and that the information is deleted once the conditions relating to the processing of the information are no longer relevant. The Committee inspects random samples and conducts searches of the DSE work register after the Secretariat has prepared the inspections. In 2009, the random checks were on several occasions followed up by questions in writing to the PST. The questions particularly concerned the grounds for the registrations, whether the service had complied with the rules relating to individual processing, written grounds for the registrations and deletion.

Initial registrations
The Committee has in 2009 noted that the service now generally follows the requirement relating to the formulation of specific work hypotheses for initial registrations in the PST work

register. The Committee will continue to focus on this requirement also in 2010. This will make it possible to assess whether the service has had sufficient grounds to record and follow up information relating to individuals.

Deletion and retention of registrations
The Committee has also in 2009 regularly conducted random spot checks of registrations to which no new information has been added in the last five years. According to the guidelines, such registrations must be deleted if they are no longer necessary to serve their original purpose.

Based on this five-year rule, the PST reviewed the registrations pertaining to a larger number of people to evaluate whether they should be retained or deleted. The Committee's random checks showed that the review had not been based upon individual assessments, something PST acknowledged when the registrations were to be submitted to the Committee. The service's new review resulted in deletion of about 80 per cent of the originally retained registrations.

The issue illustrates that it is of great significance that the PST individually assesses each work registration which is retained – and that the EOS Committee closely and regularly oversee that the service complies with the five-year rule relating to extended registrations.

Registrations based on ethnic, religious or political conviction
Section15 of the PST instructions reads: "The service can not collect information simply on the basis of what is known about a person's ethnicity or national background, political, religious, or philosophical conviction, union or association affiliation, or information about the individual's health or sexual orientation". During the review of last year's annual report, the Standing Committee on Scrutiny and Constitutional Affairs emphasised that this should continue to be a key focal area.

The Committee has asked the PST for a written report on the service's practice relating to the prohibition laid down in Section 15 of the PST instructions. What criteria or factors should be present before the service can process information about a person's political, religious or philosophical conviction? The Committee has also asked the service to clarify to what extent a person's affiliation with violent organisations or environments could constitute grounds for collecting and processing information about the person in question. Moreover, whether participation in demonstrations is sufficient for work registrations.

The issue is still under consideration and will be followed up in the annual report for 2010.

3.3 Disclosure of personal data to foreign collaborating services

PST's guidelines for disclosure of information read: "Information can be disclosed to foreign collaborating police authorities and to security or intelligence services to avert or prevent criminal acts or if it is necessary for the verification of information." Moreover, it is stipulated in the fourth paragraph that unverified information only can be disclosed if required for "important security-related reasons". In such cases, the PST must focus on the "quality and importance" of the information and "who the information is about and who is the recipient of the information". Furthermore, if the information is unverified, the service must inform the recipient of the information of this.

The Committee will check that the service does not disclose any information which may be contrary to these guidelines or to Norway's international human rights obligations. The

Committee emphasises that the service is careful not to disclose information to states that do not respect human rights.

The control routines are as follows: For each inspection, DSE presents an overview of the information that has been disclosed since the previous inspection. The Committee carries out random checks of the overview where the Committee requests to see all case papers which might illustrate the reason for the disclosure. The Committee has also carried out spot checks by searching disclosed information recorded in the service's electronic record-keeping system.

The inspection of the PST's disclosure of personal data to foreign collaborative services did not reveal any grounds for criticism of the service.

3.4 The PST's use of concealed coercive measures

The PST is permitted to use the same concealed coercive measures as the rest of the police service, including communications surveillance, electronic room surveillance and concealed room searches. Since 2005, the PST has had the authority to make use of coercive measures to *prevent* and *avert* criminal acts. The PST is the sole police authority with permission to employ coercive measures to prevent criminal acts. In 2009, the collective use of coercive measures was more or less the same as for the previous year.

The Committee has inspected whether there is congruence between the service's total information material in individual cases and the requests to the court to use coercive measures. Another key focal area is to ascertain that coercive measures are not used outside the timeframe specified by the court. The Committee also checks to see that the measure is discontinued if the suspicion or premise of the investigation is disproved. Furthermore, it has been important to verify that the service meets the Storting's condition that concealed coercive measures for pre-emptive purposes should function as a safety valve and be employed with extreme caution. Based on this, the Committee has checked that the service only uses concealed coercive measures to prevent the most serious crimes.

The 2009 inspection of the PST's use of coercive measures in individual cases has not revealed grounds for criticism of the service. *The importance of the Committee ensuring strict control of the use of coercive measures was emphasised by the Storting when the legal authority was extended in 2005. The Committee will follow up this condition also in 2010.*

3.5 The cooperation between the PST and the immigration authorities

The cooperation between the PST and the immigration authorities is currently relatively extensive. It covers the exchange of information in immigration matters, including matters pertaining to visas, asylum applications and deportation cases. In its 2008 annual report, the Committee stated that it in recent years has focused on increasing its knowledge of the collaboration between the EOS services and other public authorities. As the Committee's area of oversight is functionally defined, the Committee may also have a more direct responsibility of oversight of authorities that collaborate and exchange information with the EOS services.

PST and the Norwegian Directorate of Immigration (UDI) have for some time been preparing guidelines for how the collaboration between the PST and the immigration authorities should be implemented at various levels. UDI submitted the guidelines for this collaboration to the Committee in September. The guidelines shall "facilitate and ensure high quality and uniform exchange of information between UDI/UNE and the PST on issues where such exchange of

information is necessary". The guidelines include UDI's and UNE's contact with the PST in all individual cases pursuant to the Immigration Act and the Norwegian Nationality Act. The guidelines apply to, inter alia, the classification of information processed by the UDI/UNE, rules relating to the right of access and provisions relating to contact routines between the PST and the immigration authorities, both centrally and between the PST's local units and UDI's regional offices and reception facilities.

In the Committee's opinion, there has been an obvious need for clearer guidelines for the collaboration between the service and the immigration authorities. Through inspection of the PST in 2010, the Committee will ensure that the provisions in the new guidelines are complied with. The Committee will also organise a meeting with the UDI in 2010, at which the Directorate's collaboration with the PST will be a central topic.

3.6 Investigation of PST's sources

In its 2008 annual report, the Committee stated that it would investigate more closely the PST's use of a source/informant who may have been guilty of war crimes and violations of human rights. The case originated from a press release in November 2008 claiming that the PST collaborated with an Afghan general living in Norway to obtain information about the situation in Afghanistan. The press claimed that the Oslo Public Prosecutor's Office decided not to initiate an investigation of the general following a recommendation from the PST. During its review of the 2008 annual report, the Storting Standing Committee on Scrutiny and Constitutional Affairs asked to be kept informed about the case.

The Committee has studied the case documents to clarify whether the information submitted by the PST to the Public Prosecutor is in fact based on the information which the service has about the general. In addition, the Committee has investigated whether or not the PST made a deal with the general to refrain from investigation in return for his cooperation with the service – or whether the service's recommendation to the public prosecutor was based on the notion that an investigation would impede the service's chances of gaining information from him. *The investigations that were carried out did not provide sufficient grounds to pursue the matter further*.

The case did, however, raise some principal concerns regarding the PST's use of sources/informants that may be guilty of serious crimes, such as violation of human rights. Such matters raise some difficult deliberations regarding the scope and content of the collaboration vis-à-vis the potential disclosure of useful information in return. The situation may be that the person in question is in possession of information which is vital to the PST's ability to prevent, avert or investigate violations affecting matters of national security. On the other hand, such close cooperation may conflict with the general sense of justice. *Thus, the Committee will pay particular attention to this problem in the future.*

3.7 Supplementary grounds for persons complaining to the Committee about unlawful surveillance

During the Committee's investigation of a complaint regarding unlawful surveillance lodged against the PST, it emerged that the PST had retained information about the complainant beyond what was necessary for the purpose of the registration. This matter was not comprised by the original complaint. The PST was asked to consider the Committee's request to inform the complainant about this matter, or submit the case to the Ministry of Justice and the Police should the service be unable to provide the complainant with information on the Committee's findings and criticism (Annual Report, Ch. III.10).

The PST replied that they were unable ”to see that there are any grounds to accept the complaint lodged by A. Thus, there should be no reason to inform him about the significantly less serious matter revealed by the Committee”. In this respect, the PST referred to the Committee's criticism being related to the fact that the service had retained information about the person for a much longer period than necessary due to a technical system fault.

Thus, the PST submitted the matter to the Ministry of Justice and the Police for review. In its reply to the PST, the Ministry stated that, principally, it agreed with the Committee's assessment with respect to, inter alia, the nature of the PST's activities entailing that individuals have no basis for knowing what surveillance activities they may have been subjected to:

”Consequently, it would not be reasonable to expect that the complainant should have directed his complaint against the matters that the Committee finds questionable in order to be informed about the result of the Committee's case processing. It is the circumstances identified through the Committee's investigation that may be subject to criticism...The Ministry presumes that the information about A has now been deleted...and we acknowledge that the technical fault/obstruction has now been rectified.”

After the Ministry's assessment, the Committee received a proposal from the PST for a more detailed reply to the complainant, in which the PST states that:

”The extended retention of the information was due to a fault in the system which searches for information that is to be considered for deletion. Thus, the PST has failed to process this information in accordance with the internal guidelines for information processing. This regrettable fault has now been corrected.”

The Committee found that the PST's proposal sufficiently clarified the Committee's criticism regarding the complaint, and informed the service of this in a letter to the PST. The Committee believes the matter has yielded several key clarifications of a principal nature with regard to complainants' right to receive information about the Committee's criticism in complaint matters.

4. THE NATIONAL SECURITY AUTHORITY (NSM)

4.1 Inspections – general information about the supervision of the service

In 2009, the Committee carried out four inspections of the NSM. Furthermore, the Committee inspected the personnel security clearance service of the Ministries' Service Centre (DDS), the Norwegian Defence Research Establishment and the Ministry of Justice and the Police. In addition, inspections were carried out of the personnel security clearance service in the Norwegian Defence Security Service (FOST), cf. Chapter 5 for more details.

In 2009, the Committee received three complaints directed at the NSM, compared to one complaint in 2008. One of the complaints was directed at the PST, the intelligence service and the FOST. *The Committee has not expressed criticism relating to the closed complaints.*

In 2009, the Committee raised several issues relating to the processing of security clearances. The regulations pertaining to this have been revised in recent years. This has improved the legal protection for persons who are being vetted for security clearance through, for instance, the right to be granted grounds and access.

However, the Committee's inspections have revealed, both in 2009 and in previous years that challenges still remain with regard to safeguarding the individual's rights in issues relating to security clearances.

4.2 Issues concerning access to the minutes from security interviews

During an inspection of the NSM in May 2008, the Committee received an account of how the service conducts security interviews. Pursuant to Section 25a of the Security Act, an individual who has been the subject of a security clearance assessment shall have the right to familiarise himself with the documents pertaining to the case "once a decision on security clearance has been made". For purposes of comparison, the main rule for individual decisions in the public administration is that a party has the right to acquaint himself with the documents in the case, cf. Section 18, first subsection, of the Public Administration Act. The principle of contradiction indicates that an individual who is the subject of a security clearance assessment should be granted access to the documentation also *before* the clearance authorities have made their decision.

The Committee asked the NSM for a written account of its views on the person in question's right to familiarise himself with, and possibly comment on, the minutes from the security interview *before* the decision relating to security clearance is made. Furthermore, the Committee asked whether the NMS was of the opinion that the principle of contradiction or other considerations warrant that the person in question should have such a right. In its reply, the NSM stated that the person in question has a right to be given a reason and a right to appeal. The service was of the opinion that the individual's legal protection and the principle of contradiction were sufficiently safeguarded. Consequently, the service concluded as follows:

"The NSM thus postulates that such access may prevent the case from establishing a sufficient and truthful basis of information, which must be deemed to represent a security problem. In general, one could say that access to the clearance authorities' decision basis prior to a decision may prevent a real and individual overall evaluation of the individual's security."

The Committee agreed with the NSM that, according to the current regulations, no such access exists to the minutes from the security interview before the decision has been made. However, the Committee stated in its concluding letter to the NSM that the principle of contradiction and the case information indicate that the person who is being considered for a security clearance *should* be entitled to access into the relevant minutes from the security interview (Annual Report, Chapter IV.4).

The Committee will follow up this issue in 2010 and provide a statement in its next annual report.

4.3 Case processing in cases concerning security clearance

Case from the Norwegian Defence Estates Agency

During the inspection of the NSM in November 2008, the Committee asked to see the Norwegian Defence Estates Agency's negative security clearance decisions that had not been appealed. The Committee questioned six of the cases where no internal concurrent justification had been prepared. In four other cases, a written report had been prepared which included a justification. The report had, however, been prepared after the security interview had been conducted. In its reply to the Committee, the Norwegian Defence Estates Agency emphasised that the regulatory requirement had been complied with as the Agency

had prepared an internal concurrent justification after a security interview had been conducted.

The Committee stated the following in its concluding letter to the Norwegian Defence Estates Agency:

”The duty to prepare an internal concurrent justification is however not limited to cases where a security interview has been conducted, as the Norwegian Defence Estates Agency seems to base its views upon. The Committee therefore finds it necessary to point out that in six of the reviewed clearance cases no evaluations have been made. In the light of this, we request that the Norwegian Defence Estates Agency changes its routines for preparation of internal concurrent justifications to ensure that the case processing complies with the regulatory requirements.”

The Norwegian Defence Estates Agency subsequently informed the Committee that the clearance authority will prepare an internal concurrent justification in the future in accordance with the regulatory requirements. After this the Committee found no further reason to follow up the issue.

Following the same inspection of the NSM in November 2008, the Committee also questioned a refusal to grant access. The reason for the refusal was that the clearance case had not been appealed before access was requested. In its concluding letter to the Norwegian Defence Estates Agency relating to this issue, the Committee stated that:

”Pursuant to Section 25a, first subsection, first sentence of the Security Act, an individual who has been the subject of a security clearance assessment shall have the right to familiarise himself with the documents pertaining to the case “once a decision on security clearance has been made". The provision does not stipulate that the clearance decision must be appealed before access to the case documents can be granted. The right of access to one's own case is a fundamental prerequisite for the possibility of the individual to safeguard his interests. … The Norwegian Defence Estates Agency regretted that A was denied access into the case due to a misinterpretation of the regulations. The Committee requests that the Norwegian Defence Estates Agency informs A of the fact that the refusal was due to a misinterpretation of the regulations and that A may now have access to the clearance case."

The Norwegian Defence Estates Agency subsequently informed the Committee that the person who had been denied access, had been granted access to view the documents in the clearance case, and had been given an extended time limit to file a complaint. After this the Committee found no further reason to follow up this issue.

Case from the Ministry of Justice and the Police

During the inspection of the NSM in November 2008, the Committee was also presented with a negative security clearance decision that had not been appealed and that had been made by the Ministry of Justice and the Police. The person in question had been given the security clearance at the level ”confidential” as requested, but on the condition that the security clearance was only valid for the relevant position. The person was affiliated with another state. However, it was not clear from the case what assessments the Ministry had made regarding the person's affiliation with the foreign state.

The Committee asked the Ministry to assess why the person in question had received no information or grounds in accordance with Section 25, third paragraph, of the Security Act. Furthermore, the Committee requested that the Ministry give an account of why the security clearance was granted on the said condition. *The Ministry of Justice and the Police agreed with the Committee that a decision to grant a security clearance on certain conditions constitutes a partly negative decision, and that more detailed grounds should have been provided. The Ministry will base their views on this interpretation of Section 25 of the Security Act in similar cases.*

The Committee stated the following concerning the lack of specific assessment relating to the affiliation to another state:

”The NSM guidelines state that a specific assessment must be made of whether the affiliation may influence the person's security-related suitability, including both the nature and degree of affiliation. The country's security-related significance will also be relevant. As the case documents do not specify which specific assessments the Ministry of Justice has made in the case, and as the Ministry has not been able to specify this retrospectively, it is somewhat difficult for the Committee to assess whether the decision has been based on an individual, comprehensive evaluation.”

In the light of this, the Committee asked the Ministry to reassess the case, assuming that the complainant's affiliation with the state in question and the reason for the stipulation of the said condition would then be included in the new assessment. The Committee requested to be informed about the reassessment of the clearance case, and will follow up the Ministry of Justice and the Police's handling of this case in 2010.

5 THE NORWEGIAN DEFENCE SECURITY SERVICE (FOST)

5.1 Inspections – general information about the supervision of the service

The inspection activities
In 2009, the Committee carried out three inspections of FOST. One of the inspections was carried out at Jørstadmoen, where the centre for the protection of critical infrastructure is located. The section is a part of FOST’s information security department. During the inspections of FOST, the Committee reviews all negative security clearance decisions made by FOST since the previous inspection. In addition, the Committee inspects FOST’s files, case records and electronic systems. During the inspection at Jørstadmoen, the Committee also inspected the technical capacity of the section.

Special challenges related to FOST
Inspections of FOST have on several occasions left the impression that the service has had an insufficient understanding of the Committee's role and function as an inspection body. The Committee has, for instance, found it difficult to gain access to the service's routine descriptions of administrative procedure regarding personnel security. Moreover, insufficient presentation of cases and documents requested by the Committee in advance has made it difficult for the Committee to carry out its inspections. The Committee has also noted that the case processing time in FOST for several cases raised by the Committee in writing has been exceedingly long, also after repeated written reminders.

The Committee has raised several important issues relating to FOST’s use of intrusive methods, including the statutory basis for FOST’s inquiries and notoriety in connection with the service's operations. FOST seems to have been insufficiently aware of the legal framework of the service's activities and the importance of individual legal protection.

Consequently, the Committee welcomes the Ministry of Defence's new instructions for security service in the Armed Forces, which are under preparation. The new instructions will presumably better facilitate the Committee's inspections (Annual Report, Ch. V. 3).

5.2 The Committee's right of access to FOST

During the inspection of FOST in December 2008, the Committee was informed that routine descriptions had been prepared for the case processing in the service's personnel security department. The Committee requested that this be submitted to the Committee, a request which was denied by the service. Instead, the routine descriptions were presented to the Committee during the April 2009 inspection. The service pointed out at the time that the routine descriptions had not yet been approved by the service's management. The Committee stated that this was not relevant to the Committee's right of access. The routine descriptions were finally submitted to the Committee. The routine descriptions describe internal case processing routines for personnel security cases – related to issues such as financial circumstances, criminal offences, health conditions, substance abuse, handling of complaints, handling of access petitions and authorisations for ”restricted”. Upon submission of the communications, FOST expressed scepticism about having to submit these documents:

”In our opinion, the Committee's request to have these documents submitted for inspection seems somewhat peripheral in view of the Committee's main responsibility, which, according to the Section 2 of the Act of 3 February 1995, No. 7, last subsection, is to conduct subsequent oversight of our decisions. … We regard all routine descriptions to be dynamic documents. This means that minor and major changes and additions are continuously made to the documents as and when required. … Furthermore, FOST will not feel obliged to keep the EOS Committee updated with consecutive submission of the new and altered versions of the routines.”

In its concluding letter to FOST, the Committee specified that the Committee's responsibilities are laid down in Section 3 of the Act relating to the Oversight of Intelligence, Surveillance and Security Service which states that the Committee shall deal with all matters and factors that it finds appropriate to its purpose, including regulations, directives and practice”. Furthermore, the Committee stated that:

”The Committee's right of inspection is laid down in Section 4 of the Act relating to the Oversight of Intelligence, Surveillance and Security Service which stipulates that the Committee has an unconditional right to demand access to the services’ archives and registers. All employees of the administration shall on request procure all materials, equipment, etc. that may have significance for effectuation of the inspection.”

Moreover, the Committee specified that it expects FOST to submit any changes in the routine descriptions’ *content to the Committee. The Committee has asked FOST to confirm that the service will follow this practice in the future. The Committee has not received this confirmation, nor have we received a reply to our reminder. This is regrettable. The Committee will follow up this issue relating to FOST in 2010* (Annual Report, Ch. V).

5.3 The Committee's inspection of the use of methods in FOST

The Committee stated in its 2008 Annual Report that it had investigated three cases relating to FOST’s use of methods. Furthermore, the Committee stated that this would be addressed in the Annual Report for 2009, also requested by the Storting Standing Committee on Scrutiny and Constitutional Affairs.

The background for the Committee's inspections

In a letter to the Ministry of Defence in 2008, the NSM raised concerns regarding FOST’s use of methods within the field of security intelligence. The NSM expressed concerns regarding FOST’s investigations of a security cleared Norwegian person in military post abroad (hereinafter referred to as ”A”), of the private security sector and of the activities relating to Computer Network Defence (CND).

In a letter to the Ministry of Defence, the Committee asked whether inquiries had been instigated as a result of the NSM's letter. Based on the serious nature of what had been described and the Ministry's information that no organised inquiries were taking place, the Committee decided to instigate its own investigations. The Ministry was informed of this decision. At the same time, the Committee received the Chief of Defence's account of the issue from the Ministry of Defence.

The investigation's sources, discoveries, criticism – and the Committee's recommendations

The Committee's investigations of the case consisted of a review of documents and electronically stored material, including video and sound recordings, photos, printouts of messages from a social networking site and Word documents. The Committee also reviewed police documents and documents in a security clearance case, and conducted interviews with FOST employees and other persons familiar with the cases. Questions were also directed to FOST in writing. The Committee's report emphasises that for the purpose of oversight it is "of great significance that the services are able to document the activities, including that the service has notoriety for assessments with respect to purpose, legal grounds and exchange of information. This is particularly important when the operation involves the use of intrusive methods, and when the inspections are directed at individuals". Moreover, the Committee pointed out that FOST's consideration of what is regarded as a "matter of security" did not seem to be in accordance with the regulations, particularly in the case regarding A. In the Committee's opinion, this case should have been considered a personnel security case, and the investigations should have been left to the NSM as the appropriate clearance authority.

"FOST's insufficient awareness of this point has resulted in the service processing sensitive information about a number of people who are not relevant to the service's area of responsibility. … With respect to the individual, it is therefore important that more detailed guidelines are established for the handling of information, including collection, systematisation, retrieval, disclosure, deletion, etc."

Remarks from the Ministry of Defence and the Committee's preliminary conclusions

On 17 June 2009, the committee submitted a classified report on the investigation to the Ministry of Defence and FOST. The Ministry of Defence commented on the three issues investigated by the Committee in a letter sent to the Committee in November 2009. With regard to the issue relating to the private security sector, the Ministry stated that it is unacceptable that FOST neither replied to the Committee's request for comments, nor submitted documents concerning the source of the case.

In its reply to the Ministry of Defence, the Committee stated:

"The Committee has noted that the Ministry of Defence has observed that both the Chief of Defence and FOST have failed to provide sufficient information about the cases, and that in some instances incorrect information has been provided about circumstances that are important to the Committee's investigation of the cases. The Committee would again like to point out that it is essential for the purpose of oversight – and to the legitimacy of the service's activities – that the supervisory body is provided with sufficient and correct information. The Committee considers the failure to do so a very serious matter indeed."

The Committee will keep itself informed of the Ministry's further follow-up. The Committee will closely follow up the issues raised in connection with the cases during its inspections of FOST in 2010 (Annual Report, Ch. V.3).

5.4 Access to FOST's instructions

In the spring of 2009, the Committee was contacted by the Norwegian television channel TV2. The TV channel requested access to the Chief of Defence's instructions to the head of FOST. The reason for the request was that the Ministry of Defence had denied TV2 access to the instructions, on the basis that the instructions were classified as "restricted". FOST later declassified the instructions and granted TV2 access. However, TV2 still asked the Committee to consider the original refusal and the basis for the classification of the instructions.

In a letter to the Ministry of the Defence, the Committee requested to be informed of the reason why TV2 had been denied access to the instructions, including the statutory basis for the refusal and why the instructions had been classified. The Committee also asked why the instructions had subsequently been declassified. The Ministry replied that the service had classified the instructions after the receipt of the access petition as it was not desirable to expose the service's capacity within military counter intelligence. The Committee replied to this statement in a new letter to the Ministry:

"According to the instructions, FOST has been given the executive responsibility for the military counter intelligence. However, the instructions do not state what capacity the service has within military counter intelligence or what personnel are involved in these activities. It is, therefore, somewhat unclear to the Committee why it was felt that the capacity and personnel might be exposed if access to the instructions was granted. … As the Committee has been informed of the fact that the instructions have now been declassified and made public, the Committee sees no reason to follow up this issue further."

In a subsequent letter from the Minister, the Ministry of Defence agreed with the Committee that there had been no reason to classify the instructions. The Ministry added that the new instructions for the security service in the Armed Forces, which are being prepared by the Ministry, will not be classified but be made available to the general public.

5.5 FOST's processing of security clearance cases

During the Committee's inspections of FOST, the Committee carries out random spot checks of the service's negative security clearance decisions. On the basis of these inspections, the Committee raised several issues in 2009. (Annual Report, Ch. V.6).

Use of telephone conversations in cases relating to financial matters

The Committee questioned the service's use of telephone conversations in cases relating to financial matters and asked whether the services deemed it "obviously not necessary" to conduct security interviews in such cases, Cf. Section 21, third paragraph, of the Security Act. After having received information about the general practice in FOST, the Committee stated the following:

"Cases involving financial difficulties are often complicated. This means that the person in question should be given the opportunity to present his or her case in a security interview. The person may then make the necessary preparations and will be able to offer an explanation in a relaxed atmosphere. In addition, he or she will have the opportunity to attend together with an assessor. … The fact that FOST deliberately applies a different practice than other clearance authorities is also unfortunate. Consequently, the Committee requests that FOST review its use of security interviews in cases concerning financial matters."

After nearly one year, the Committee has still not received a reply from FOST and will follow up this matter in 2010.

Stipulating the length of the observation period
The observation period is the earliest time a security clearance case can be reassessed after a negative security clearance decision has been made. The observation period must not exceed five years, and is binding for other clearance authorities.

On the basis of the Committee's review of negative security clearance decisions from FOST, the Committee asked what assessments the service makes in cases relating to financial matters. The Committee also questioned why the length of the observation period varied in the individual cases inspected by the Committee. Also in connection with individual cases relating to drunk-driving, the Committee had reason to question why the length of the observation period varied.

In the light of the Committee's questions relating to the length of the observation period, FOST stated, after a reassessment, that the observation period should have been the same in all cases except one. The Committee had no comments to this, but noted that the case indicates varying practices in the service.

Authorisation to collect financial information
FOST has informed the Committee about a new routine for processing financial information in clearance cases. The routine entails that the person who is subject to a security clearance assessment must sign an authorisation granting FOST the right to collect more detailed financial information about that person than what is stated on the personal data form. According to FOST, security clearance will not be implemented in cases where this procedure is not followed. This raised several questions of principle, which the Committee found reason to comment on:

”Even though information regarding financial problems is stated on the personal data form it hardly entails that the clearance authority should conduct a more detailed assessment of the situation in all cases and that it thus will need more detailed information of the individual's financial situation. A practice where FOST routinely requires authorisation to set aside the duty of secrecy in such cases will consequently constitute an intrusion and would violate the principle stipulated in Section 6 of the Security Act which states that the means and methods used shall involve no more interference than appears to be necessary. … The Committee therefore requests that FOST raise the issue relating to the use of authorisations with a view to clarifying how this should be done in practice. The Committee has requested to be informed as soon as this has been done.”

The committee will follow up the issue in 2010.

5.6 Complaint relating to access in security clearance case – and case processing time

In 2007, one person, ”A”, filed a complaint with the Committee relating to FOST’s rejection of his request for access to his dismissed security clearance case. The Committee criticised FOST’s extended case processing time and emphasised the need for speedy processing of such access petitions. FOST did not submit a reply accounting for its decision until almost 18 months later. The service then partly accepted the complaint relating to both the security clearance decision and the access decision. As regards the case processing time, FOST stated that the reason for the delay was due to a replacement of the officer in charge, and because of the exceedingly extensive, complex and challenging nature of the case.

The service did not comment on the Committee's request to grant the complainant access to the correspondence with the Committee in the case, but stated the following in a letter to the complainant:

”We have also noted that the EOS Committee practically promised you access to these documents in their correspondence in the case. We regret that the EOS Committee's statement has raised your expectations of being granted access to these documents. The fact that your security clearance case has been discussed by the EOS Committee as a separate case, and that our statement in that respect is a document in the case, does not change the fact that these documents belong to FOST as the issuer of the documentation. … With reference to the above, declassification or access to the documents including our statements to the EOS Committee, will not be considered.”

In a letter to FOST of October 2009, the Committee stated the following:

”On the basis of the service's statement, the Committee has found reason to point out that in a complaints case, a processing time of more than 18 months is highly unsatisfactory. When the service's initial processing time is approximately 18 months to two years, one should be able to expect that the service would prioritise the case upon receipt of a complaint, to avoid inconveniencing the complainant further. As the Committee pointed out in its letters of 3 March 2008 and 25 November 2008, a speedy case processing is particularly important in cases concerning access petitions, as it greatly affects the person in question's opportunity to maintain his or her own interests in the appeal case...

Despite our repeated requests, of 3 March 2008, 27 May 2008, 25 November 2008, 17 February 2009, 10 March 2009, 27 April 2009 and 17 June 2009 respectively, the Committee has still not received a reply from FOST regarding the request for access to the document. The Committee has, however, through submissions from the complainant, learned that the service has denied access to the letter as it does not constitute a part of ”the case documents” according to Section 25 a of the Security Act. In the Committee's view, it is very difficult to see how one can fail to regard the document as a part of ”the case documents.”

The Committee further requested that the remaining correspondence between FOST and the Committee be declassified, so that the complainant could receive a copy of the correspondence as soon as possible.

The Committee has still not received a reply from the service. This is highly regrettable, particularly in the light of FOST's extended processing time, both relating to the clearance case and the complaint made to the Committee. FOST's handling of these cases raises doubt about the service's respect and appreciation for the individual's legal protection, as well as for the Committee's oversight responsibilities and control function. The Committee will follow up FOST's handling of the case closely in 2010, and provide a detailed account of the case in our next annual report (Annual report, Ch. V.7).

6 THE INTELLIGENCE SERVICE

6.1 Inspections – general information about the supervision of the service

The Committee has carried out three inspections at the Intelligence Service headquarters. Furthermore, is has carried out two other inspections of the service's technical procurement activities. In 2009, the Committee received five complaints directed at the Intelligence Service, all of which were also directed at PST. One of the complaints was also directed at NSM and FOST. This case is still under investigation. All cases have been investigated in the service. *The Committee has not expressed any criticism in the closed cases.*

During the inspection of the Intelligence Service, the Committee has prioritised inspection of the technical procurement activities which the service performs. A technical expert has assisted the Committee during the inspection.

6.2 Joint operation between PST and the Intelligence Service

As described in our two previous annual reports, the Committee has investigated a joint operation involving PST and the Intelligence Service. The investigation into the role of the Intelligence Service concerned the legal basis on which it played out its role in the operation. During its review of the 2008 Annual Report, the Standing Committee on Scrutiny and Constitutional Affairs requested to be kept informed of the Committee's investigations.

The Committee has concluded its work on the case. The issues raised by the Committee concerned the legal basis for the service's role in the operation, including the relationship to Section 4 of the Intelligence Service Act and the routines for political approval of the service's methods and operations. The Intelligence Service evaluated and found the operation to be in correspondence with the legal basis of the service, given that it concerned international terrorism, thus falling within the core area of the statutory responsibilities of the service. Furthermore, the service stated that the operation was directed at activities abroad and not at Norwegian citizens. The Intelligence Service stated, inter alia, the following:

”The joint operation was carried out in the interest of both the Intelligence Service and the PST. The Intelligence Service's operational purpose and focus were exclusively directed at foreign (external) affairs. Pursuant to Section 4 of the Intelligence Service Act, the procurement in this specific case did not take place ”on Norwegian territory”. In this connection, we refer to the dialogue and correspondence between the EOS Committee, the service and the Ministry of Defence relating to the general interpretation of Section 4 of the Intelligence Service Act. The Intelligence Service cannot see that any unfortunate connections have been made in this case with regard to the legal basis of the Intelligence Service and PST respectively. The division between national and international intelligence has been maintained in this case.”

In the closing stages of the case, the Committee stated that it is important in joint operations to consider the legal basis thoroughly in advance, and that the services inform each other of any legal impediments in its own regulations. As the actions that were taken could in law and in fact be assessed in different ways, the Committee found reason to express some caution in its conclusion (Annual Report, Ch. VI.2).

The Intelligence Service subsequently stated the following in a letter to the Committee:

”The Intelligence Service agrees that there were doubts as to whether the principle of legality had been observed with regard to this action...Nuances in the actual circumstances may, however, be significant to the legal assessment of the action, as stated by the Committee.
- - -
The service has in retrospect reviewed and improved the internal routines to ensure that this is maintained in future joint operations."

The case has clarified important matters of principle, and the Committee will continue to focus on oversight of the collaboration between the services.

6.3 Supplementary routines for the collaboration between PST and the Intelligence Service

The supplementary routines for the collaboration between the two services were adopted on 14 October 2009. The purpose of routines is first and foremost to specify the collaboration between the services. This can apply to, for instance, the relations with foreign collaborating services and authorities, exchange of information, analysis collaboration and mutual assistance in individual cases and specific operations. The routines shall primarily regulate forms of collaboration which require clarification with regard to the services’ respective legal basis or that are of a principal importance. The routines shall ensure that there is a focus on notoriety and re-examination in the exchange of information.

The Committee welcomes the enhanced regulation of the collaboration that has now been established between PST and the Intelligence Service. The Committee will continue to oversee that the routines are complied with, and that they provide a sufficient basis for maintaining individual legal protection within all areas of the services.

6.4 Exchanging information with foreign collaborative services

The Intelligence Service Act stipulates that one of the responsibilities of the Intelligence Service shall be to procure information about international terrorism. The service therefore collaborates with foreign intelligence and security services. During its inspections, the Committee will conduct searches and random spot checks of messages sent by the service to foreign services. The service will then assess whether it needs to make exceptions to the Committee's access in order to protect its sources. If this is the case, the Committee will be informed about the type of information withheld by the service and the justifications for withholding it.

A main control point for the Committee is to ascertain whether the service upholds the injunction stipulated in Section 4 of the Intelligence Service Act. The Act stipulates that the Norwegian Intelligence Service shall not "on Norwegian territory monitor or in any other covert manner procure information concerning Norwegian physical or legal persons". The service may, however, hold information concerning Norwegian citizens when such information is directly associated with the statutory duties of the Norwegian Intelligence Service. Consequently, it is the Committee's responsibility to check how procured information and requests for information about Norwegian citizens are handled by the service. The current practice is that information procured about Norwegian citizens is either deleted or forwarded to the PST. The Committee checks the information which the service forwards to the PST, and that the service does not disclose information about Norwegian citizens to foreign collaborative partners.

The Intelligence Service has established a system for internal control which will identify any breaches in the internal routines, also with regard to the exchange of information with foreign collaborative services. The service will in this connection strengthen its internal training.

The Committee will keep informed about the service's internal control in 2010 and aims to conduct more regular inspections of the service's exchange of information with foreign collaborative services in the future. The Committee's inspections of the service's exchange of information with collaborative services have in 2009 not revealed grounds for criticism.

6.5 The Committee's inspection of the service's technical information procurement

During the 2009 inspections of the service, the Committee has emphasised the oversight of the technical procurement activities. The main purpose of the inspection is to ensure that the service does not, on Norwegian territory, monitor Norwegian citizens, cf. again Section 4 of the Intelligence Service Act.

In 2009, the Committee established new inspection routines to oversee the service's technical information procurement: The Secretariat will to a greater extent than previously involve the Chair of the Committee and the Committee's technical expert in the inspection preparations. This will result in a more thorough and relevant inspection of the service's technical information procurement.

In 2009, the Committee has observed that the Intelligence Service is continually working to develop its capacity and methodology for technical information procurement. Moreover, the

processing and analysis tools for processing the information are continually being updated and developed. The service has throughout the year kept the Committee continually informed of any developments. The service has had an open and accommodating attitude.

Inspections carried out in 2009 of the Intelligence Service's information procurement have not revealed instances where the injunction against surveillance of Norwegian legal persons has been violated. Nor has the Committee revealed any other grounds for criticism in connection with its inspection of the technical information procurement activities of the Intelligence Service.

The EOS Committee

Street address
Akersgata 8, third floor. (Entrance from Tollbugata)

Postal address
Stortinget, 0026 OSLO

Telephone number
+47 23 31 09 30

Fax number:
+47 23 31 09 40

E-mail
post@eos-utvalget.no

Web site
www.eos-utvalget.no