Annual Report 2008

The Norwegian Parliamentary Intelligence Oversight Committee (the EOS Committee)

Preface

Pursuant to the Act relating to the Monitoring of Intelligence, Surveillance and Security Services of 3 February 1995 no. 7, the EOS Committee submits a report outlining its activities to the Storting every year. The Annual Report for 2008 is structured in the same way as previous years. Chapter I provides a brief introduction to the Committee's mandate and composition. Chapter II contains an outline of Committee activities in 2008 and accounts for the main aspects of overseeing the services, completed inspections, and investigated complaints and other matters raised on the Committee's own initiative. In addition, the report describes the Committee's contact with other public authorities and foreign oversight authorities. The exchange of experiences between oversight authorities is essential for developing expertise in an area to which the general public does not have access.

Chapters III – V account for the overseeing of the services, both the inspection activities in general and matters of principle the Committee has brought to the attention of the services. Experiences from 2008 have shown that Committee activities contribute to safeguarding the rights of the individual, as well as generating the general public's confidence in that the services operate within their legal framework.

When the Committee's annual report for 2007 was up for review in the Storting, the Standing Committee on Scrutiny and Constitutional Affairs requested that the Committee return with a further briefing on the follow-up of certain matters. These matters have been included in the annual report, with reference to the Standing Committee's request in the relevant sections.

Chapter VI outlines the Committee's proposed amendments to the Act and Instructions. Chapter VII concerns administrative matters. Appended to the report are documents containing information about the Committee, the Act relating to the Monitoring of Intelligence, Surveillance and Security Services, and the Instructions for Monitoring of Intelligence, Surveillance and Security Services, as well as a letter to the Storting regarding proposed amendments to the Act and Instructions.

Table of Contents

Pursuant to Section 8, no. 2 of the Act relating to the monitoring of Intelligence, Surveillance and Security Services of 3 February 1995, No. 7, the Committee's reports to the Storting shall be unclassified. Under provisions of current legislation, 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.

I. MANDATE AND COMPOSITION

1. The Committee's mandate

The EOS Committee's mandate is contained in the Act of 3 February 1995, No. 7 relating to the Monitoring of Intelligence, Surveillance and Security Services (the EOS Act) and in the Instructions for Monitoring of Intelligence, Surveillance and Security Services (the EOS services), stipulated by the Storting resolution of 30 May 1995 (the EOS Instructions). The EOS Committee is responsible for continuous oversight of the intelligence, surveillance and security services performed by the public authorities, or under management of or on commission from the public authorities. A provision is contained in Section 30 of the Act of 20 March 1998, No. 10 relating to Protective Security Services and Section 6 of the Act of 20 March 1998, No. 11 relating to the Norwegian intelligence service referring to the EOS Act which stipulates that the Services shall be subject to the Committee's oversight.

The Committee's most important task is to prevent injustice against any person during the practice of intelligence, surveillance and security services, cf. Section 2 of the EOS Act. The Committee shall also carry out a general oversight of the legality of the services, as the provision further states that the services be kept within the framework of statute law, government directives and non-statutory law.

The primary policy instrument of the oversight activities is inspections of the Services' archives, computer-based systems and installations of any nature, cf. Section 11, No. 2 of the EOS Instructions. The oversight of individual cases and operations shall normally abide by the principle of subsequent oversight and should be arranged in such a way as to interfere as little as possible with the day-to-day activities of the services, cf. Sections 4 and 7 of the EOS Instructions. When exercising its right of inspection, the Committee shall consider what is necessary for purposes of oversight and observe consideration for protection of sources and of information received from cooperating services abroad.

The Committee shall examine all complaints from individuals and organisations, cf. Section 3, second subsection of the EOS Act. Any complaint or request where a person or organization claims to be subjected to unjust treatment shall be investigated in the services against which they are directed.

2. Composition of the Committee

The Norwegian Parliamentary Intelligence Oversight Committee has seven members, including the chairman and vice-chairman. Deputies are not elected. The members are elected by the Storting in a plenary session on the recommendation of the Storting's Presidium. The term of office is normally five years. The members may be re-elected.
The Committee conducts its day-to-day work independently of the Storting, and members of the Storting are not permitted to simultanously 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 is currently chaired by *Helga Hernes,* Senior Adviser at the International Peace Research Institute in Oslo (PRIO), and former state secretary at The Ministry of Foreign Affairs and ambassador to Vienna and Bern. Deputy Chair is *Svein Grønnern,* Secretary General of SOS Children's Villages in Norway and former Secretary General of the Conservative Party. The other Committee members for the year 2008 are: *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 Minister of Agriculture and member of the Storting (Labour Party), *Knut Hanselmann*,

mayor of Askøy Municipality and former member of the Storting (The Progress Party) and *Theo Koritzinsky*, Associate Professor of Social Studies, Oslo University College, former member of the Storting and Chairman of the Socialist People's Party.

Kjersti Graver passed away 14 February 2009. She was a Committee member from May 29, 1998 and was re-elected til 30 June 2009.

An overview of the Committee member's terms of office (when the member was elected for the first time and when his/her term of office expires):

Helga Hernes, Oslo, chair	8 June 2006 - 30 June 2009
Svein Grønnern, Oslo, deputy chair	13 June 1996 - 30 June 2011
Kjersti Graver, Bærum	29 May 1998 - 30 June 2009 († 14 February 2009)
Trygve Harvold, Oslo	7 November 2003 - 30 June 2011
Knut Hanselmann, Askøy	8 June 2006 - 30 June 2011
Gunhild Øyangen, Agdenes	8 June 2006 - 30 June 2011
Theo Koritzinsky, Oslo	24 May 2007 - 30 June 2009

II. OUTLINE OF COMMITTEE ACTIVITIES IN 2008

1. Main points regarding the inspection of the services

The Norwegian Police Security Service (PST): Prompted by a specific complaint, the Committee has raised issues with PST and the Ministry of Justice and the Police of whether individuals should be able to gain access to information about themselves in the service's archives and registers and of the standards one should expect from public authorities in dealing with petitions for access. Personal information stored in PST's archives and registers are largely classified, and thereby also subject to secrecy, and may also be subject to secrecy for other reasons. However, PST should still have procedures ensuring that any petition for access should be subject to a specific assessment of issues related to declassification and, if applicable, public access. Administrative procedures of this kind, which follow from provisions in applicable legislation and regulations, must be adhered to, even though access to personal information stored by PST will rarely be granted. The Committee has emphasised its position on this matter to the service and the Ministry of Justice.

Upon inspection of a joint operation, involving PST and the Norwegian Intelligence Service, the Committee concluded that there were some doubts as to whether PST had applied a court order to seize mail in accordance with the purpose of the order and the provisions of the Criminal Procedure Act. The Committee also criticised the service for failing to inform the court of its motivations for seizing a specific mail shipment.

The Norwegian National Security Authority (NSM): The Committee's inspections of the National Security Authority has in 2008 not revealed any specific matters that warrant further investigation or any procedural insufficiencies within the service. The Committee has become aware, however, that certain matters were handled by the operative security department of the Armed Forces' Security Section (FSA), which was renamed the Norwegian Defence Security Service (FOST) as of 1 January 2009. The Committee has investigated the matter thoroughly, and questions have been raised as to the methods available to the FSA in collecting information about matters and incidents threatening national security.

The Norwegian Intelligence Service (NIS): On a specific matter regarding a request for information on a Norwegian citizen from NIS to PST, the Committee concluded that there must be a clear distinction between collecting information through covert intelligence

operations on Norwegian soil and exchanging information between the services. The Committee did not find grounds to criticise the service for its actions on this specific matter, but the investigation contributed to the clarification of important issues in the application and interpretation of the Intelligence Service Act.

2. Inspection activities

Pursuant to Section 11, no. 2 of the EOS Instructions, the Committee's inspection activities must, at minimum, include six inspections every year at PST' headquarters, quarterly inspections at NSM and semi-annual inspections at NIS headquarters. In addition, the Committee must inspect PST units in at least four police districts, at least two external units of NIS and/or security and intelligence functions at military headquarters or units, and at lease two security clearance authorities outside NSM.

These requirements were all met in the inspection activities of 2008. The Committee has in 2008 carried out a total of 26 inspections, of which six were carried out at PST's Central Unit (DSE), four were carried out at NSM, and three were carried out at NIS headquarters. 13 inspections covered local offices of the services, including three inspections at FSA. The Committee's technical expert participated in seven of the inspections completed.

During the year, the Committee has organised 17 internal committee meetings to, inter alia, plan and follow up on inspections. In addition, part of the Committee also organised a meeting in DSE.

The following external units and local offices were inspected in 2008: PST Søndre Buskerud, PST Salten, PST Østfold, PST Vest-Finnmark, the Norwegian Post and Telecommunications Authority, the Norwegian Petroleum Directorate, the PST Personnel Security Service, the Joint Operative Headquarters (FOHK), the Regional Command in Northern Norway (LDKN), and the vessel F/S Marjata.

3. Complaints and matters investigated on the Committee's own initiative

The Committee received 13 complaints in 2008, compared to 22 in 2007. All complaints were directed at PST. One of the complaints also included NIS and NSM.

Throughout the year the Committee investigated 13 matters on its own initiative.

4. Meetings and visits

MEETING WITH THE DATA INSPECTORATE

In February 2008 the Committee organised a meeting with the Data Inspectorate wherein issues related to the administration of personal information were discussed. The collection and handling of personal information for national security reasons is normally exempt from oversight from the Data Inspectorate. However, there will always be certain areas, in terms of privacy, where the responsibilities of the Data Inspectorate and the Committee come into contact.

During this meeting issues relating to the proposal for new legislation on police registration and the regulations relating to PST administration of personal information were discussed as well. The Data Inspectorate gave an account of the EU data retention directive of 2006. Pursuant to current regulations, Norwegian telephone operators and internet service providers are obligated to retain traffic data for three to five months for invoicing purposes. The new directive orders operators and service providers to retain communication data for a minimum of six months and a maximum of two years for purposes other than invoicing. This directive entails an expansion of the kinds of personal information operators and service providers are obligated to retain, including information on base stations used in mobile telephone communication.

MEETING WITH THE DUTCH REVIEW COMMITTEE ON THE INTELLIGENCE AND SECURITY SERVICES

The Committee was in April 2008 visited by the Dutch Review Committee on the Intelligence and Security Services. This Committee's mandate is to review the legality of activities in the Dutch intelligence and security services. Their area of oversight is, as for the EOS Committee, functionally defined and not linked to specific organisational units. The Dutch committee is independent of the Dutch Government and Parliament and has, by law, been granted substantial discretion to complete its responsibilities.

In addition to an information meeting with the Committee, meetings with the Standing Committee on Scrutiny and Constitutional Affairs, PST, and NIS were arranged. In meeting with the Dutch committee, the EOS Committee gave an account of its mandate and oversight activities in general, and the parties discussed problems related to the administration of personal information and special challenges related to oversight activities.

MEETING WITH THE VENICE COMMISSION

In June 2008, the President of the Venice Commission, Associate Professor Jan Helgesen with the Norwegian Centre for Human Rights, and the Norwegian representative in the Venice Commission, Professor Fredrik Sejersted with the Centre for European Law, briefed the Committee on the commission's mandate and activities. The Venice Commission is an advisory body on constitutional matters and general issues related to the rule of law in nations.

The Committee was briefed on the commission's report on democratic oversight of security services. This report accounts for various oversight models and also provides examples of good practice from oversight authorities in various countries. The parties also discussed problems related to extraordinary rendition and the detention camp in Guantánamo Bay.

OFFICIAL INAUGURATION OF THE SWEDISH COMMISSION ON SECURITY AND INTEGRITY PROTECTION

The Committee Chair and Secretariat participated in the official inauguration of the Swedish Commission on Security and Integrity Protection in June 2008. Representatives of the Portuguese and Dutch oversight authorities were also present during the reception. In connection with the inauguration, a meeting with the representatives of the various oversight authorities was organised.

MEETING WITH THE REVIEW COMMITTEE FOR POLICE MEASURES

Committee members and the Secretariat Chair met with the Review Committee in September 2008. This committee was appointed by the Government, inter alia, to review the amendments of 2005 on the investigative use of coercive measures by the police, including provisions on communication surveillance, wire taps, and the use of coercive measures for preventive purposes. The EOS Committee Chair gave an account of the Committee's oversight activity of the use of concealed coercive measures by PST. Both technical challenges in the overseeing process and challenges related to the Committee's inspection activities were discussed, as well as problems related to the disclosure of information to collaborating services and assessments as to the scope of surveillance.

SEMINAR IN STOCKHOLM ORGANISED BY THE SWEDISH COMMISSION ON SECURITY AND INTEGRITY PROTECTION

In December, the Committee Chair and Secretariat Chair participated in the *International Symposium on National Security and the European Convention on Human Rights* in Stockholm, organised by the Swedish Commission on Security and Integrity Protection. The Committee Chair gave a presentation on the right to an effective remedy pursuant to Article

13 of the European Convention on Human Rights and contributed the Committee's assessment as to whether Norway satisfies the requirements for an effective remedy in the Committee's area of oversight.

MEETING WITH SLOVAKIAN PARLIAMENTARY COMMITTEE
A delegation from the Slovakian parliamentary committee for oversight of military intelligence visited the Storting in December 2008. Their visit included a meeting with the Committee to discuss parliamentary oversight of intelligence, surveillance, and security services.

5. Seminar regarding oversight of international intelligence collaborations

In October 2008 the Committee organised an international conference entitled "Accountability of International Intelligence Cooperation" in collaboration with the Geneva Centre for the Democratic Control of Armed Forces (DCAF) and the Human Rights Centre at the University of Durham. As the Committee has previously reported, international collaborative operations involving security and intelligence services from different nations are increasing, especially in the field of counter-terrorism. This trend is highly challenging for oversight authorities in most countries, because the international intelligence activities are regarded as highly sensitive by the services, and efforts to inspect such activities are often frustrated, because the legislation and regulations to which oversight authorities are subject normally do not grant them access to information received from foreign services. The increase in international intelligence collaboration has raised concerns about the effects such collaborative operations may have on the respect for human rights and the right of the individual to protection under the law. The objective of the conference was to highlight challenges related to oversight of collaborative international intelligence operations, as well as to discuss different ways to improve accountability for such collaborative operations.

In addition to problems related to the exchange of information between security and intelligence services, challenges associated with terror listings, extraordinary rendition, and participation in international military operations were key topics during the conference. Various national oversight models were accounted for, including how oversight activities are organised in the different countries and which opportunities and limitations arise in inspecting such joint operations. Ideas concerning supranational oversight bodies were also discussed, and examples of national and international investigations were presented.

Representatives from the oversightauthorities of other nations, international organisations, and the Norwegian EOS services participated in the conference, as well as members of academia. Conference papers will be collected and published. In addition, there are plans to issue a manual or frame of reference regarding oversight of the collaborative operations of the EOS services across national borders.

III. THE NORWEGIAN POLICE SECURITY SERVICE (PST)

1. Inspections, in about the supervision of the service

In 2008, the Committee carried out six inspections at DSE. In addition, inspections were carried out at local PST units in Søndre Buskerud, Salten, Østfold, and Hammerfest.

The Committee received 13 complaints directed at PST from individuals in 2008, compared to 18 complaints in 2007. All complaints were investigated centrally at PST headquarters, as well as in local units when the Committee found reason to do so. None of the investigations found any grounds for criticism.

In 2007, the Committee reported that it, in connection with a specific complaint, had addressed certain issues regarding the interpretation and application of the provisions of the Freedom of Information Act and the Security Act with PST and later the Ministry of Justice

and the Police. PST records and documents are exempt from public disclosure in their entirety. In addition, this information is normally classified pursuant to the Security Act. However, when petitions for access to documents are submitted, the legislation to which the services are subject requires that a specific evaluation into declassification and public access be made.

The Committee is contacted by many people who have had their petitions for access to information about themselves in PST's archives and registers denied. In addition, the Committee receives complaints from individuals where the issue of access is involved. Making sure that classification is not used where there is no real need and that the issues of declassification and public access are evaluated in accordance with regulation requirements are important oversight responsibilities. On this basis, the Committee has investigated whether PST's practice is in accordance with the regulations. This matter is further addressed in Section 3 below.

In 2007 the Committee reported on its investigation into a joint operation involving both PST and NIS. As part of this investigation, the Committee raised the issue of how coercive measures, if necessary, could be used in this context, and, more generally, of which rules to apply. This specific matter was not described further, as the investigation was still ongoing, but the Committee emphasised that the investigation up to that point indicated a need to further evaluate the regulations to which the collaboration between services are subject.

The Committee continued its investigation in 2008. A key issue has been the scope of powers granted to PST by a court order on the use of concealed coercive measures, when this court order is issued as part of the service's preventive activities. The specific case concerned a court order to seize a mail shipment. Another key issue was whether the court was sufficiently informed of the motivations for using the coercive measure. This matter is further addressed in Section 7 below.

2. Inspection of archives and registers

2.1 Introduction

Inspecting PST archives and registers has continued to be a key part of the Committee's oversight activities in 2008. During each inspection at PST headquarters, the Committee inspects the service's intelligence register, SMART, and its administration and record keeping system DocuLive. This is accomplished by the Committee reviewing random samples based on various types of searches made by the Secretariat prior to the inspection. The central aspect of this activity is to make sure that PST does not unfairly collect and retain personal information on individuals and that the service does not retain information that is no longer necessary and relevant.

An "intelligence registration" is, in Section 1-2, no. 7 of the Regulations concerning PST's collection of information, defined as the "collection and retention of information regarded necessary in order for PST to complete its tasks, that does not warrant the establishment of or inclusion in a preventive matter." The inspection of PST registration procedures is centred on the requirement that a specific and individual assessment must be completed for each registration, both in terms of the quality of the available information and the operative relevance thereof. The Committee must determine whether the justification revealed and the factual information on which the registration is based meet the conditions of necessity, relevance, and a clear purpose, as established by the PST Instructions. PST guidelines have established more specific conditions for the collection and retention of information by PST, which has meant that the Committee in 2008 has been able to carry out a more targeted inspection of the service's archives and registers than previously possible. In 2008 the Committee has also questioned the basis on which a number of intelligence registrations have been made. This matter is further addressed in Section 2.2.

The Committee has in 2008 continued its practice of inspecting random samples among the intelligence registrations retained past their five-year evaluation. This inspection specifically targets the deadline for reassessment, how the discretionary exclusionary provision is put into practice and that the reason for the continuation is apparent from the intelligence register. Based on the random samples taken for this purpose, the Committee has, on a general basis, addressed the practice of retaining registrations in the counter intelligence field after five years with PST. This matter has yielded certain useful and fundamental clarifications and will be further described in Section 2.3 below.

When PST implemented a new, integrated intelligence register for the entire service in March 2005, it was on the condition that all former manual and electronic intelligence registers, even in local units, would be discontinued. In its last three annual reports, the Committee has pointed out that some local units have kept their local intelligence registers, which is contrary to the guidelines issued by PST headquarters. During its inspections in 2008 the Committee has once again revealed an operative local intelligence register. This matter is further addressed in Section 11.

2.2 Individual registrations and the service's practice regarding the requirement of completing an individual evaluation prior to registration

During the year, the Committee has called several of PST's intelligence registrations into question on the basis of findings from random samples taken from the intelligence register SMART. In certain cases, the Committee has requested that the service provide a more detailed justification for the decision to collect personal information about individuals, due to the difficulty of ascertaining from the registered information whether there are sufficient grounds for an intelligence registration. Furthermore, the Committee is concerned about whether the service meets the requirement of completing an individual assessment prior to collecting information on individuals. This issue has been a priority in inspections in recent years. The Committee has, in these cases, been particularly interested in whether the collection and retention of information meets the conditions of necessity, relevance, and a clear purpose, in accordance with Sections 13 and 14 of the PST instructions.

In 2008 the Committee has also in certain cases taken issue with registrations that appear to be in breach of Section 15 of the PST instructions that 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".

Following questions from the Committee after sample inspections, the service has carried out a new evaluation of its registrations and has since elected to delete or amend information in the intelligence register.

The regulations relating to the service's collection and retention of information on individuals and the guidelines established in December 2007 help clarify the limits for inclusion of information on individuals in the intelligence register. The PST instructions and the new guidelines have also been of significance for the Committee's inspections of the service's collection and retention of personal information. With a more distinct framework, the Committee is better able to evaluate whether the service's practices are justifiable. The Committee will continue to focus on the registration practices of PST.

In 2007 the Committee reported that PST was in the process of developing an internal review system, as part of its obligations in accordance with Section 16, Subsection 1 of the PST instructions, cf. Chapter 6 of the guidelines. This internal review system will, as far as the Committee has been informed, be completed in 2008.

2.3 Evaluation of intelligence registration in the field of counter intelligence

The Committee has in 2008 continued its practice of regular inspections of random samples from the intelligence register that have been retained past the five-year evaluation. Section 3-7, Subsection 3 of the guidelines requires a review of intelligence registrations that have not been amended in five years, and the entry must be deleted if the information is "no longer necessary to serve its purpose". Decisions to retain intelligence registrations must be made by the head of the PST, or the person authorised by him, and the decision must be made in writing. The Committee especially checks to see that the time limit for re-evaluation is upheld, assesses how the service uses discretion in retention decisions, and makes sure that the grounds for retention are clear from the intelligence register. The consequence of a retention decision is that the registration will be retained for another five years.

In 2008, the Committee has raised some general concerns about the service's procedures for carrying out five-year evaluations within the field of counter intelligence and questioned the retention of certain registrations past the five-year mark within this field.

In its response to the Committee, PST referred to current regulations, in which service operations related to illegal intelligence activities are justified. The service stated that the five-year evaluations are based on the discretion of police experts, and that this discretion will vary slightly according to the field under which each registration sorts. PST stated that a long-term perspective is of vital importance within counter intelligence, a statement which the service also previously had pointed out to the Committee. Furthermore, the service gave a detailed account of the various considerations that come into effect in this field when it comes to evaluating the possible retention of registrations after five years.

As to the concerns about the individual registrations raised by the Committee, PST responded that the registrations in question had been reviewed, and that it, following a specific evaluation, was no longer deemed necessary to retain these.

In closing the issue, the Committee pointed out that the background on which the matter was addressed with the service was that the Committee had learned that in counter intelligence activities there is often an expressed need to retain registrations on a somewhat longer timeframe than is the case in other fields.
The Committee expressed its understanding for the needs of the service to retain intelligence registrations within this field on a longer timeframe, and made reference to PST's statements that the assessments will be based on the discretion of police experts.

However, the Committee still found it necessary to emphasise the importance of the service carrying out a specific assessment in each individual case when registrations are retained. Furthermore, the Committee presumes that the service carries out an individual assessment of the grounds for registering information on an individual in this field for every new registration, particularly given the risk that this information may be retained in PST's intelligence register for a long time. The Committee made reference to Section 14 of the PST instructions, which states that information registered should not be retained longer than what is necessary to serve its purpose, as well as to the aforementioned condition in Section 3-7, Subsection 3 of the guidelines, concerning the five-year evaluation.

In closing, the Committee made the following remarks:

> "The Committee holds that the account here given about the service's practice in matters of this kind has contributed to important clarifications, and the Committee's future oversight activities will be based on this understanding. The matter raises some difficult questions and considerations that the Committee believes would be best resolved in connection with the

investigation of individual matters. In its future oversight activities, the Committee will thus pay particular attention to these problems.

In terms of the individual registrations that formed the basis for the Committee's questions to the service, the Committee has noted that specific evaluations of the individual objects concluded that retaining said objects is to no longer necessary to serve the original purpose of their registration. The Committee thus expect these registrations to be deleted."

2.4 Inspection of topical archives and personal information archives – transfer to National Archives

The Committee's inspection of PST's topical archives and personal information archives in 2008 has not revealed any practices that has prompted further follow-up of the service. As far as the Committee has been able to ascertain, the service has reviewed and sorted cases and documents that have no relevance for the field, and reviewed material prepared for shredding or transfer has been stored separately from other archive material.

In its 2007 report, the Committee informed that the PST shredding stop, which was implemented on the basis of the temporary review arrangement for the service, was abolished. This entailed transferring irrelevant material from the service to the National Archives. In 2008, the Committee has kept informed about the service's transferral activities.

Prompted by the abolishment of the shredding stop, the service implemented a project in the summer of 2007 concerning the transferral of paper documents from the period between 1945 and 1994 to the National Archives. Electronic registrations from before 1994 are, according to the service, copied into a database connected to the intelligence register SMART, but which is not in operational use. Archive material from the period between 1994 and 2005 will be transferred collectively at a later date. The transfer entails that the National Archives will assume responsibility for the documents. Provisions concerning the transfer of public archives can be found in Section 10 of the Archive Act, cf. Section 5-7 forward of the Archive Regulations.

Pursuant to Section 2-5 of the Information Safety Regulations, classified material shall remain classified for 30 years from the date of classification, unless otherwise specified. The National Archives presumes that PST specifies which documents shall remain classified past this period. If the National Archives are approached about access to PST documents in the possession of the National Archives, PST will be contacted for a specific assessment of classification issues, in that the service is the issuing agency. The National Archives will determine, pursuant to provisions on confidentiality in the Public Administration Act, whether there are grounds to uphold confidentiality for documents that have not been classified. In the main, the period of confidentiality is 60 years, pursuant to Section 13c of the Public Administration Act. However, pursuant to Section 11 of the Public Administration Act, the National Archives may prolong the period of confidentiality if personal circumstances so dictate. The National Archives have informed PST that they will carry out specific evaluations to determine whether or not there is a need for such measures. If so, the period of confidentiality is normally prolonged to 80 years.

Due to space limitations at the National Archives, PST has not yet commenced the transfer of material to the National Archives. The service has informed the Committee that the transfer will commence in the fall of 2009 at the earliest. Over the course of 2008, DSE has begun collecting documents for transfer from local units. This material will undergo an evaluation by DSE before it, if applicable, is transferred to the National Archives.

In 2009, the Committee stay informed of PST's efforts to transfer material to the National Archives.

3. PST procedures for dealing with requests for declassification and access

In last year's report, the Committee accounted for a general matter addressed with PST and the Ministry of Justice regarding the right to access PST archives and registers and the procedures regarding petitions for access. A specific complaint brought this matter to the attention of the Committee. The complainant had requested access to any information about her deceased father, about whom she believed the service had registered information. Her petition had been denied without any justification, and without informing her of her right to appeal the decision to the Ministry of Justice pursuant to the Freedom of Information Act. When the ministry investigated the complaint following a request from the Committee, it too denied the petition, and informed the complainant that the provisions do not grand the citizen party rights in terms of access to PST registers.

A central issue in this matter concerns the requirements in the information safety regulations for a specific assessment concerning declassification of classified information. Another key issue is the application of the principle of public access in PST matters. In its 2007 report, the Committee stated that it would continue to work on these issues in 2008, and in its review of last year's report, the Standing Committee on Scrutiny and Constitutional Affairs requested that it be informed of the results of the Committee's investigations on this matter.

To the Committee's questions in 2007 about how the provisions of the Security Act concerning declassification and procedures regarding petitions for access should be applied by PST, as well as how procedures for applying the principle of public access and the right to appeal decisions to deny access should be practiced, PST had the following, primary reply:

> "Even though the public administration regulations, Part V, no. 14 make exceptions for access to PST archives, one should still consider granting access based on the principle of public access. In cases where it is deemed appropriate to grant the applicant access to information from PST archives and records, it naturally follows that an assessment of a possible declassification of information in accordance with Section 2-13 of the information safety regulations is carried out immediately following this decision.
>
> If the service deems the principle of public access to be relevant in a specific case, the assessment of a possible declassification of information must be carried out in accordance with the provisions of Section 2-13 of the regulations on information safety. In cases where the service does not grant access to the requested information, it would not be expedient to obligate the service to complete the added task of evaluating declassification of the documents in question."

PST regretted that it had not previously had procedures in place to inform applicants of their rights according to Section 9, Subsection 4 of the Freedom of Information Act to appeal decisions to deny petitions for access, and informed the Committee that this would be done in the future. As a consequence of this response, the Committee referred the complaint in question to the Ministry of Justice as the proper appellate authority, and requested that the Ministry review the complaint. The Ministry rejected the complaint. The Ministry stated that as a main rule, party rights in the form of access are not granted "in accordance with PST archive guidelines". In its letter to the Committee of the same date, the Ministry noted the following, with reference to the distinction between a party's right of access pursuant to Section 18 of the Personal Data Act and rights of access pursuant to the Freedom of Information Act:

> "In terms of PST there are no expressed provision regarding party right of access, however it is generally accepted that the registered party does not have such rights. This has been established in several public documents, the most recent being the Official Norwegian Report NOU 2003:21 on Crime Prevention and the Right of Personal Privacy, cf. especially the sections concerning PST and access to personal information in Items 4.21.7 and 23.6.2.1. The

> proposed act concerning the registration of personal information by the police and public prosecuting authorities (Police Registry Act) includes a specific chapter on PST (Chapter 8), which in Section 60 states that the provisions concerning duty of disclosure (Section 43) and right of access (Section 44) do not apply to PST. This entails that once the new police registry act takes effect, individuals registered in PST registers will not have right of access. Comments to this proposal have been invited, but at this point no objections have been submitted.
>
> The Ministry is of the opinion that the issue of applying the principle of public access must be seen in light of these developments. There would be no continuity in the system if, on the one hand, PST registers are exempted for party right of access, while subjecting the same information to the principle of public access on the other hand. Exemption from party right of access, thus automatically entails that access cannot be granted under the provisions of the Freedom of Information Act. The principle of public access will thus never be a relevant issue for personal data stored in PST's intelligence registers, etc."

In response to this, the Committee addressed several issues concerning access to PST archives and registers in letters to the Ministry. The Committee agreed that no *rights* exist, granting access to the service's archives and registers, but it questioned whether a consequence of this necessarily would be that the principle of public access would not be applied in processing specific petitions for access. The Ministry was also asked to account for its views on whether the purpose of exempting PST journals and documents from public access pursuant to the Freedom of Information Regulations also entails an exemption from the duty to consider public access pursuant to the Freedom of Information Act. Finally, the Committee asked how PST would relate to the provisions of the Security Act, with regulations, when receiving petitions for access or declassification, specifically Section 2-13 of the information safety regulations. This provision obligates the service to carry out an evaluation of whether or not information can be declassified when petitions for access to classified information are submitted.

In its response to the Committee, the Ministry gave an account of the issue of individual access to PST archives and registers in several documents, where it, inter alia, stated that the existing regulations do not grant such access. Furthermore, the Ministry made reference to how an individual does not have the right to access information about whether or not that individual has been under surveillance/registered, cf. Section 8, no. 1 of the Act relating to the Monitoring of Intelligence, Surveillance and Security Services. On the latter, the Ministry stated:

> "This principle entails that in its reply to petitioners for access, the service will neither be able to confirm nor deny whether the individual is registered in PST archives or registers. However, the Ministry concedes that the replies given by PST may be insufficiently constructed, so that the petitioner is not given the necessary information as to why access is denied. The Ministry will therefore, in collaboration with PST, seek to formulate a reply that better explains and justifies this arrangement."

Furthermore, the Ministry pointed out that the Storting on several occasions has considered the issue of access to the service's archives outside of the provisions of the temporary Disclosure Act, but that this issue has not gained majority approval in the Storting. The Ministry believed this illustrates that the temporary provisions of the Disclosure Act was regarded as an exception for a limited time only, and concluded that "one should not allow for right of access to the archives of the Norwegian Police Security Service – not even in connection with older cases".

As regards unclassified documents, the Ministry stated that an evaluation into the principle of public access could be relevant, and agreed with the Committee that the aforementioned provision in the Freedom of Information Regulations does not entail a general exemption

from the duty to consider the principle of public access. As regards the issue of which procedures to apply to petitions for access to classified information, cf. Section 2-13 of the information safety regulations, the Ministry stated that considering issues of declassification and the possible application of the principle of public access *simultaneously* was unlikely to be in violation of the regulations, provided that the same agency was responsible for carrying out both assessments. The Ministry further stated:

> "The Ministry will consider whether there is a lack of coherence between the provisions of Section 2-13 of the regulations on information safety, which seem to presuppose that the individual requesting access to classified information has the right to receive a reply, and the fact that the issue of whether or not information about an individual has been registered by PST is regarded as classified information, which, for obvious service-related reasons, can neither be confirmed nor denied."

The Committee found it necessary to ask certain follow-up questions to the Ministry regarding the principle of public access in petitions for access to unclassified, including declassified, documents. The Committee furthermore requested a more detailed account of what the Ministry meant with its statement that the information safety regulations are no obstacle to considering the issues of declassification and the principle of public access "simultaneously".

In its reply, the Ministry confirmed that "an evaluation into the principle of public access must be carried out in connection with unclassified documents". The Ministry further stated:

> "In Item 2 [of the Committee's letter] one questions whether it is possible to carry out an assessment into the principle of public access while simultaneously considering the issue of declassification. By simultaneously the Ministry refers to the situation where this assessment, for practical reasons, is carried out during the time period during which the matter is under consideration by the same agency, but that one, in this process, first makes a decision on the issue of declassification and then decides on the principle of public access.
> In cases where another agency has issued the information, and thus is responsible for deciding on the issue of declassification, one must first contact this agency for a decision on the issue of declassification before the issue of public access can be considered by the recipient agency of the petition for access. This situation may be different if the issuing agency is subordinate to the agency considering the petition for access and thus is subject to general instruction authorities, cf. the regulations on information safety, Section 2-11."

The letter from the Ministry also stated that the Ministry had not decided whether the issue of access should be considered differently in connection with older cases.

In its concluding letter to the Ministry, the Committee stated:

> **"1.**
> In inspecting PST, the Committee is particularly concerned with making sure that the service's procedures for administering data on individuals correspond to the provisions for administering personal information to which the service is subject. Recently, the Committee has received several complaints and petitions concerning access to the service's archives and registers. The Committee believes this raises several key questions, where many conflicting considerations must be taken into account. The Committee has found it useful to hear the views of the service and the Ministry on this matter, and the Committee believes the matter has yielded several key clarifications of a principal nature.
>
> **2.**
> The Ministry has, on several occasions, emphasised that no *rights* exist, granting access to PST archives and registers. The Committee agrees that it, in the case of PST, is not expressed right of access to information collected by the service. On the other hand, there is no expressed provision that, on a general basis, precludes access to PST archives and registers. However, information stored by PST is largely classified, and thus subject to a

statutory duty of secrecy. As the Ministry has also pointed out, the information is also, as a general rule, exempted from public disclosure, pursuant to Part V of the regulations relating to the Freedom of Information Act (currently Section 9, Subsection 3 of the Freedom of Information Act).

The Ministry also pointed out that it follows from the proposed Police Registry Act that the right of access shall not apply to PST. However, the Committee would like to stress that the point of departure, for PST as well other public agencies, must be that a petition for access must be subjected to a specific evaluation, even though PST in practice will grant access in significantly fewer cases than what is the case for other administrative agencies. In this context, the Committee further points out that Section 60 of the proposed Police Registry Act regarding exemptions from the provisions of Sections 43 and 44 on the duty of disclosure and the right of access does not entail an exemption from remaining provisions on which procedures to apply in considering petitions for access, cf., in PST's case especially, Section 2-13 of the regulations on information safety and the provisions of the Freedom of Information Act, with pertaining regulations.

3.
For the Committee, the key issue in this matter has been to determine which procedures PST must consider in receiving petitions for access, especially including the significance of the principle of public access to the administration. The Committee has noted that the Ministry has concluded that the principle of public access may be considered in cases involving unclassified documents, after previously stating that public access "[will] never be a relevant issue for personal information stored in PST's intelligence registers, etc.".

A key issue is what the provisions of Section 2-13 of the information safety regulations entail in cases when PST receives petitions for access. Subsection 1 of the Section reads as follows:

> "In cases involving petitions for access received by the issuer of classified information, the issuing agency shall, without undue delay, consider whether the information in its entirety, or parts thereof, may be declassified, cf. Section 2-10. Access shall be granted to any declassified information, unless statutory provisions preclude access under or pursuant of the Freedom of Information Act or other statutory provision."

The Committee has taken this provision to mean that the issue of classification must be considered before one can consider whether or not access must or ought to be denied on another basis. In the opposite case, any considerations as to whether information may be exempted from access on another basis would be superfluous if the information cannot be declassified. The service arrived at the opposite conclusion in its letter to the Committee of 5 March 2007, whereas the Ministry, in its letter of 11 June 2008, believed the issues of declassification and possible public access could be considered "simultaneously". The Committee does not agree with this interpretation, but took note of the Ministry's clarification in its letter of 16 November 2008, responding to the Committee's letter of 8 September 2008, in which the Committee addressed this point. The Committee has no objections to the assessments being carried out "in the time period during which the matter is under consideration by the same agency", in the words of the Ministry, provided that one reaches a conclusion on the issue of declassification before, if applicable, moving on to consider the principle of public access, unless there is a statutory provision on the duty of confidentiality exempting the information from access. In this regard, reference is made to the following statement in the remarks to Section 9, Subsection 3 of the regulations pertaining to the Freedom of Information Act, cf. the draft legislation of 17 October 2008 concerning the implementation of the Freedom of Information Act (Implementation Bill), which, inter alia, states:

> "If the information in question is not classified or subject to confidentiality on any other basis, one must still consider the principle of public access in general, pursuant to Section 11 of the Freedom of Information Act."

This will be the situations in which PST, on the basis of an access petition, conclude that the information to which access is requested may be declassified, cf. Section 2-13 of the regulations relating to information safety.

…

4.
The Committee is aware that issues concerning access to PST archives and registers in many ways are different from issues concerning access to information administered by most other administrative agencies. The majority of information is classified, and thus confidential, and will for many other reasons be subject to confidentiality or be exempt from public disclosure as well. Also, individuals petitioning for access to information about themselves collected by the service will in most cases not know whether or not the service has gathered information about them. The latter is also, as previously stated, regarded as classified information.

As mentioned above, the Ministry states, in its letter of 16 November 2008, that it has not yet concluded whether issues regarding access to PST archives and registers should be assessed differently when they concern older cases. In this regard, the Committee notes that several of the considerations indicating that one should not grant access to the information stored by the service, such as concerns about methodology and current operative activities in general, is not as relevant for older cases. For the period between 1945 and 1996, the temporary disclosure arrangement has entailed disclosing information from the service to individuals and the public through media attention, etc.

It is the Committee's opinion that the threshold for granting access to older information generally ought to be lower than for information of a more recent date. This will, however, be dependent on the nature and relevance of the information, how old the information is, and the operational needs of the service to protect itself form external parties gaining access. In this context, the Committee also feels compelled to emphasise that the main rule of classification is a period of 30 years, pursuant to Section 2-5 of the regulations relating to information safety. The Committee assumes that in cases where the information is no longer deemed classified due to the period of time that has passed, there will, in many cases, no longer be other operative concerns indicating that the information should remain confidential or exempt from disclosure under the principle of public access.

As regards the period between 1945 and 1994, which was covered by the temporary disclosure arrangement for PST, the Committee is aware that parts of the PST archives will be transferred to the National Archives, and that, in cases concerning petitions for access to this material, PST will assess the issue of declassification and the National Archives will consider whether a duty of confidentiality based on concerns of personal privacy preclude access. The Committee will continue its close inspection of activities in connection with the transferral of this material and issues concerning access thereto.

The Committee believes there are many arguments in favour of considering whether one should grant, on a more general basis, access to older information collected by the service. Similar arrangements have been established, as far as the Committee is aware, in other countries, such as the Netherlands, Switzerland, and Sweden. One possibility could be to expand rights to access to information 30 years and older, cf. the aforementioned main rule for a period of classification. This type of access would, if implemented, also be applicable to information about whether or not an individual has been the subject of "surveillance activities". In this context, reference is made to the following statement from the Danielsen Committee (NOU 1998:4, p. 151):

> "Current provisions also allow for the possibility that POT or its superior authority may grant access, in special cases, to matters other than criminal cases through the declassification of documents and access to information about whether an individual has been the subject of surveillance or registration, given the presence of strong indications that the petitioner ought to have access to such information." (emphasis added)

In the Committee's view, the current regulations allows for the possibility that, in considering the classification issue in connection with an access petition, one may also consider declassifying information that an individual has *not* been the subject of surveillance or registration by the service, so that this information may be disclosed, for example if the access petition specified a certain timeframe and/or requests access to information that date back some time. One could, in such cases, disclose that PST up to a certain date has not collected any information about the individual. In line with the Ministry, the Committee believes that there may be a lack of coherence between the requirements of the provisions of Section 2-13 of the regulations relating to information safety and the fact that it is considered classified information whether or not information about an individual has been registered by PST. The Committee assumes that the Ministry will review this matter, as stated in its letter to the Committee of 11 June 2008. The Committee asks to be informed of the Ministry's decision once this evaluation is complete.

In the Committee's opinion, PST must, despite many indications against granting access to the service's archives and registers, in all cases provide the petitioner with a reply as complete and justified as possible, if the petition for access cannot be granted. The Committee has noted that the Ministry acknowledges possible shortcomings in the way PST's rejections to petitions of access are constructed, given that the information about whether or not information about an individual has been registered in PST archives and registers is regarded as classified information. The Ministry has, in this regard, stated that it, in collaboration with the service, will "seek to formulate a reply that better explains and justifies this arrangement". The Committee asks to be informed about any activities that are carried out in this respect as well.

In its letter of 16 November 2008, the Ministry states that documents pertaining to the post-war treason trials have been transferred to the National Archives, and that it "in writing to individuals [will] account more closely for how individuals may contact the National Archives, and what a petition in such cases should contain". The Committee asks to be sent a copy of this letter for its information.

5.
In cases where the Committee are contacted in connection with, or receive petitions for, access to PST archives and registers, the Committee will refer the individual to the service. If the petition for access submitted to the service is denied, the individual may appeal this decision to the Ministry of Justice and the Police, and PST now expressly informs the petitioner of this right if petitions for access are denied. If the Ministry upholds PST's decision to deny access, a complaint may be lodged to the Committee. In such cases, the Committee has the authority to carry out a post-decision inspection of the procedures applied to this specific petition for access. The Committee's authority in such cases is unique, in that the powers of other authorities, such as the courts and the Data Inspectorate, are limited when it comes to cases concerning access to classified information.

In addition to reviewing individual cases concerning access to PST archives and registers, the Committee will continue to emphasise issues of classification, including, especially, issues concerning declassification, as well as more general issues related to disclosure of and public access, etc., to the service's archives and registers. The Committee assumes that these issues are also of concern for the Ministry, in connection with the ongoing efforts to implement the new Police Registry Act, inter alia."

The Committee asked the Ministry to respond in accordance with its recommendations, and the Committee will return to this issue in its next report.

4. The concepts of registration and deletion in PST's intelligence register

In its 2007 report, the Committee accounted for specific issues concerning the concepts of registration and deletion as applied to information in PST's intelligence register SMART. In its review of the 2007 annual report, the Committee was asked to keep the Storting informed of developments on this issue.

One of the issues the Committee addressed with PST was whether the stipulations in the PST Code of Practice allows the service to use intelligence information associated with an individual after this individual has been deleted as an object in the intelligence register. The Committee became aware of this issue following inspections of random samples from SMART, when it revealed that information about individuals deleted as objects in the register was retained if the individual was mentioned in an incident concerning one or several other individuals who had not been deleted. For a more detailed description of this issue, reference is made to the account in paragraph 3 in Chapter III of the 2007 report.

As described in last year's report, the Committee concluded that the stipulations in the PST Code of Practice does not allow that the service retain intelligence information about an individual if said individual has been deleted as an object in the register. On this basis, the Committee requested that the service review the issues raised by this case, and, if necessary, initiate necessary amendments to its procedures or Code of Practice.

In its response to the Committee, PST stated that it had tried to find a practical solution to this problem, but that this has proven difficult. The service stated that the problem will be reported to the Ministry of Justice, with the objective of considering whether it is possible to clarify the existing stipulations, so that individuals that are only mentioned in the free text of entries are not subject to the requirement of a five-year evaluation pursuant to the stipulations for the processing of personal information in Section 3-7, Subsection 3 of the PST Code of Practice.

The Committee notes that the service has concluded that the stipulations must be amended, as it has proven difficult to change the practices of the service. The Committee presupposes that the service has carried out a thorough evaluation as to the possibilities of changing its practices, if necessary by implementing technical adjustments, as an alternative to amending the provisions to which the service is subject.

On a general basis, the Committee notes that one should exercise great caution when amending the stipulations of the service's Code of Practice concerning the processing of personal information, when such amendments are justified by technical or other challenges associated with the enforcement of said stipulations. In this regard, the Committee emphasises that the concern for the rights of the individual in terms of personal privacy must be fundamental in PST's processing of information in the service's intelligence register, which routinely involves the registration of sensitive personal information without the knowledge of the individual in question.

The Committee will keep informed of further developments in this matter, and in its future inspection of PST the Committee will continue to emphasise the practices associated with the service's deletion of intelligence registrations.

5. Disclosure of personal data to foreign collaborating services

In its 2007 report, the Committee gave an account of its inspection of DSE's disclosure of personal data to foreign collaborative services. In its review of the report, the Standing Committee on Scrutiny and Constitutional Affairs requested that the Committee's inspection activities concerning the disclosure of personal data to foreign collaborative services be continued.

In 2008 the Committee continued its practice of carrying out regular spot checks of DSE's disclosure of personal data to foreign collaborative services. The established inspection routine entails that DSE at each inspection provides the Committee with an overview of what has been disclosed since the last inspection. From this overview random checks are carried out, where the Committee requests to see all the documents pertaining to each case, which might illustrate the reason for the disclosure. In 2008, the Committee also carried out spot

checks by searching disclosed information recorded in the service's electronic record-keeping system.

The random spot checks carried out in 2008 did not reveal any grounds for criticism of the service. The disclosure of personal data by the service to foreign collaborative services is substantial, particularly within the framework of a bilateral exchange of information. This type of collaboration usually involves more comprehensive and detailed information about individuals, and generally also more sensitive information, than is the case in multilateral collaboration. As previously described, the Committee's rights to review are limited, because information from collaborative partners in general is regarded as highly sensitive. In certain cases, where the Committee has sought to carry out a comprehensive investigation, the service has provided the Committee with information to the greatest extent possible

In its 2007 report, the Committee gave an account of the new PST guidelines for processing information, which stipulate the conditions on which information from PST may be disclosed to collaborative services. These guidelines include, inter alia, provisions on the requirement that the purpose of disclosing the information must be seen in relation to the consequences of disclosing them. Even though the new guidelines leave a lot of room for discretion, the stipulations facilitate for better external control on the part of the Committee.

In 2008 the service notified the Committee of a preventive investigation within the field of counter terrorism, wherein information was disclosed to foreign collaborative services. PST had information prompting suspicion that a group of individuals were planning to execute a terrorist act in the near future. By gathering intelligence in this case, PST received information that the individuals were planning to travel abroad, and the service considered contacting the collaborative services of foreign nations.

Following a thorough evaluation, PST disclosed information to a collaborative service. This service assessed the severity of the suspicion, the human rights situation of the country in question, and any consequences to the individuals involved, including the potential risk that family members of the individuals in question might be in danger. The service also considered other possible courses of action on this matter, but based on the circumstances of this case it was deemed necessary to contact the service of another nation. However, PST did not find the human rights situation of this country satisfactory, and the information was thus not disclosed to this nation's service.

In its 2006 report, the Committee stated that Norwegian authorities are obligated, under the provisions of the Human Rights Act, to "secure any individual within its jurisdiction the rights and liberties" established in the European Convention on Human Rights, cf. ECHR, Article 1. This also includes the obligation to ensure that no other entities infringe upon these established rights. Disclosing sensitive personal data to nations that do not respect human rights would entail that Norway has failed to uphold its obligation under the Convention. The Committee did not reveal any grounds on which to question whether the disclosure of information in the case in question was in violation of ECHR or PST guidelines concerning the disclosure of information. The service gave a detailed account of its actions, which demonstrated that the service was aware of the problems raised by this case. Prior to disclosing information, the service carried out a specific evaluation of the necessity of disclosing the information, who the recipient of the information was, and the potential consequences for the individuals involved.

6. PST's use of concealed coercive measures

In its 2007 report, the Committee gave an account of PST's use of concealed coercive measures, for example in the form of communications surveillance, electronic room surveillance, or room searches. As of 2005, PST was given the authority, as did the police in

general, to use coercive measures during an investigation to pre-empt criminal acts – and not as previously, only to solve crimes. In addition, PST, as the sole police authority, was permitted to use coercive measures outside of an investigation, to *prevent* criminal activity.

The Committee has in 2008 supervised the use of coercive measures in individual cases. Oversight activities include reviewing the collective basis of information in specific cases to make sure this corresponds to motions in court. Another key focal area is to ascertain that PST uses the coercive measure in accordance with the court order – generally that the coercive measure is not used outside of the timeframe specified by the court. The Committee also checks to see that the measure is discontinued if the premise on which it was implemented is no longer present, for example if the suspicion or premise of the investigation is disproved.

The collective use of coercive measures is another key focal area for the Committee. Also, the Committee has made sure that the service does not initiate investigations including coercive measures for pre-emptive purposes in cases that in reality are preventive in nature, and that the service only uses invasive coercive measures to prevent the most serious crimes, in accordance with the Storting's condition for introducing the new statutory provisions in 2005.

In 2008, the Committees inspection of the service's use of coercive measures in individual cases has not given grounds for criticism of PST. The collective use of coercive measures is still modest, and in 2008 the Committee has seen a decrease in the use of coercive measures, compared to previous years.

As previously described, inspection of PST's use of concealed coercive measures is challenging, and requires that the Committee review individual cases. However, the service is highly aware of the limitations on the use of coercive measures posed by the Criminal Procedure Act and the Police Act. The Committee has also noted that PST's motions in court to use concealed coercive measures have been thoroughly substantiated, which facilitates for better external control on the part of the Committee, inspecting the service's use of coercive measures.

7. Joint operation between PST and the Intelligence Service

In its 2007 report, the Committee informed the Storting of its inspection of a joint operation between PST and the Intelligence Service. The specific operation was not described in detail because the investigation was still on-going, but the Committee stated that the investigation thus far indicated a need to review the current regulatory framework for joint operations between services. In its review of the report, the Standing Committee on Scrutiny and Constitutional Affairs asked that the Committee request the Government to review and evaluate the regulations in question.

In 2008, the Committee has continued its inspection of the joint operation between PST and the Intelligence Service. The operation in question involved PST using a current court order for mail inspection in a preventive counter terrorism case to give the Intelligence Service access to a specific shipment to serve its own purposes. The shipment was later returned to the mail system for dispatch to the addressee abroad. This matter was addressed with both PST and the Intelligence Service. Issues related to the part played by the Intelligence Service in this operation has been described in Chapter V, paragraph 3.

The issues addressed with PST concerned the scope of the court order for mail inspection pursuant to the Criminal Procedure Act, and whether the court received sufficient information about the purpose of seizing that particular shipment. Certain other issues related to the interpretation of the seizure provisions were addressed with the service as well.

In its response, PST made reference to the matter being reviewed by the service's Operational Security Committee, which upon considering the legal issues concluded that the dispositions made vis-à-vis the Intelligence Service would be authorised in law. PST informed the Committee that the court had been informed of the general purpose of the preventive case, but the court had not been informed of the joint operation with the Intelligence Service, which was tied to a specific shipment, of which PST became aware through the continuous mail inspection. PST stated that when the service was issued a court order authorising seizure of the mail shipment, this proved that the nature of the shipment was relevant in the preventive terrorism case. Furthermore, the service stated that the framework for preventive mail inspection in this case must be interpreted in a wide sense, i.e. to prevent terrorism, and that the joint operation with the Intelligence Service was regarded as falling within this legal framework, established by the court order together with the provisions of the Criminal Procedure Act relating to preventive coercive measures. PST argued that the operation stayed within this legal framework, even though the court order specifically related to the inspection of mail shipments to and from A, whereas the joint operation, which was the direct precursor of the specific seizure, related to B, who was the addressee of the shipment in question. B was a foreign national residing abroad.

On these grounds, PST concluded that the service had provided sufficient information as a basis on which the court could conclude whether the shipment was relevant to the case on which the court order authorising mail inspection was based. This is a review the court must carry out for each shipment the police/PST want to seize during a continuous mail inspection.

PST also stated that it was clear from the provisions of the Criminal Procedure Act that the powers of the prosecuting authority do not preclude the transfer of the shipment in question to the Intelligence Service in the present case. PST further stated that it generally aims to present the court with all the necessary information, so that the court may make its decisions on as comprehensive a basis as possible, but that it in this case was prudent to refrain from informing the judge, given that the matter involved a preventive operation that was highly classified, as well as especially sensitive in that it also included the Intelligence Service. PST also stated that their considerations took into account the fact that the Intelligence Service "has substantial powers under the Intelligence Service Act outside the jurisdiction of the courts".

In its concluding letter to the service, the Committee referred to Section 212 of the Criminal Procedure Act, which states that the court must open and review the seized material and assess the presumed significance of the shipment for the case. The purpose of this provision is to avoid that the police, in inspecting mail shipments, gains information outside of the purpose of the measure, i.e. to secure evidence in the ongoing investigation, cf. Proposition No. 35 to the Odelsting (1978-1979) p. 177. The Committee presumed that in mail seizures for preventive purposes, this provision must be understood as the requirement that the information must be relevant for the ongoing investigation. Furthermore, the Committee pointed out that the stipulation that the judge must open the shipment in question and assess the significance of the information for the case was established for the purposes of due process of law, and that this consideration only can be upheld by providing the court with sufficient information on the purposes of the seizure, on which the court may carry out a sound assessment of whether the shipment contains information relevant to the investigation.

The Committee stated that the provisions of Section 212 represent a guarantee for the due process of law in the application of the coercive measure, in that the court must review the shipment before granting access to the police, and that this is constructed as an absolute requirement that can only be realised if the police provides the court with sufficient

information about the purpose. The Committee could not see that the type of considerations invoked by the service in this case made it prudent to refrain from providing the court with information about the actual purpose behind the seizure. The Committee stated that it, in preventive cases, could be deemed sufficient that the court is made aware that the purpose of the investigation is to prevent terrorist activity, and that the evaluation pursuant to Section 212 would then have to be adjusted, but the Committee is of the opinion that the extraordinary use of the coercive measure in this case was indicative of a more stringent duty to inform the court. The Committee thus criticised the service for failing to provide the district court with the informational basis required by the Criminal Procedure Act.

As regards the fundamental issue of whether the seizure order could be used for the purpose of this case, the Committee referred to the provisions of Section 211 and 212 of the Criminal Procedure Act, which grants limited access of the individual shipments to the police. The access, or authorities, must correspond to the “purpose of the seizure”. The Committee assumes that this, in a preventive case, must be understood as a reference to the framework of the case, i.e. the authorities granted must be relevant in terms of clarifying the actual circumstances described in the motion before the court and/or in the court order.

The Committee stated that it could not see that the seizure provisions, including the aforementioned limitations in access, enables the police to allow another authority to gain access to, and dispose of, individual seizures for their own purposes. This will quickly result in a situation where the reality is that access to a shipment is used for purposes outside the framework of the case. This is true even if the other authority were to have the legal authority to execute the seizure itself. The Committee thus does not find it sufficient that the seizure fell within the purpose of the case – to prevent terrorist activities – when shipment was disposed of in the manner described.

When the responsibilities of PST and the Intelligence Service overlap, as is the case within the field of counter terrorism, it is especially important that the services operate strictly within their respective legal authorities. Otherwise the result will be grey areas, wherein courts run the risk of not receiving sufficient information about the actual purpose behind the coercive measures, which ultimately may result in the services as a whole being granted authorities with a wider scope than the government intended. Section 7 of the cooperation regulations for the Intelligence service and PST, stipulated by Royal Decree of 13 October 2006, facilitates for increased cooperation in specific cases following an assessment of the “separate legal authority” of the individual service. For the purposes of due process of law this is a key provision. In its concluding letter to PST on this matter, the Committee concluded that it, upon having reviewed the matter as a whole, found that PST, given the powers granted in accessing this specific shipment, had not fully complied with the court order and the provisions of the Criminal Procedure Act relating to seizures.

The Committee stated that it is highly significant for its oversight activities that there, in joint operations between the services, is a high level of clarity and notoriety surrounding the purpose and legal basis of the operation, as well as the distribution of tasks and exchange of information between the services. The Committee further noted that there seemed to be insufficient coordination between the services in connection with the legal issues raised by this operation, cf. also Section 1, letter e and Section 7, Subsection 2 of the aforementioned cooperation regulations.

Summary of the Committees views

This case illustrates the challenges that may arise when trying to join two very different legal authorities, as is the case here, especially when one is not geared towards operative activities in this country. As pointed out in the 2007 report, the Committee sees the need to initiate a review and evaluation of the regulations relevant for joint operations between the

two services. The situation will often be that obvious considerations of efficiency associated with the safeguarding of national security conflict with considerations of the individuals rights to due process of law. To the greatest extent possible, legislation or other legal provisions should balance these considerations. The Committee has learned that the services has prepared a proposal for amendments to the procedures applicable to the collaboration between the services in accordance with Section 4 of the cooperation instructions, which is currently being considered by the Ministries of Justice and Defence. In its oversightactivities, the Committee will in the future pay particular attention to whether these amended procedures are sufficient, or whether there is a need for further evaluation and review of the legislative and regulatory provisions that apply to this type of collaboration.

8. The cooperation between PST and customs authorities

In its 2007 report, the Committee accounted for a case involving a collaborative effort between PST and the customs authorities. The Committee had raised certain general questions with the Directorate of Customs and Excise regarding the accountability of its collaboration with PST and the legal basis for said collaboration. The Committee also raised the issue of two specific customs inspections carried out on the request of PST.

The Committee investigation in this case has revealed that the customs authorities are not authorised to carry out customs inspections outside “the customs administration area”, which entails that the customs authorities must independently assess whether they have the legal authority to act on requests from PST. As regards the two specific customs inspections, the Committee found that the customs authorities after the fact were unable to document the information from PST that formed the basis for its decision to carry out the inspections. This lack of documentation was criticised by the Committee. Upon further inspection at PST, the Committee found that the service, in one of the cases, had obtained a court order for the concealed search of the suspect’s luggage, but the search that was carried out was more substantial than the court order authorised. In the other case, the Committee learned that PST had not provided customs authorities with sufficient information as to what the case involved, nor was there anything in the documents pertaining to the case indicating that the suspicion held by PST was related to customs legislation.

Furthermore, the Committee emphasised the need to establish guidelines for the collaboration between PST and customs authorities. In its 2007 annual report, the Committee made reference to a signed collaborative agreement between PST and the Directorate of Customs and Excise, which states, inter alia, that any collaboration and exchange of information must take place within the respective legal bases of the parties. At that time, no guidelines had yet been developed. In reviewing the 2007 annual report, the Standing Committee for Scrutiny and Constitutional Affairs requested that the Committee follow up on this matter and return with a more detailed account.

PST has informed the Committee that guidelines for the collaboration between PST and customs authorities have now been developed, establishing, inter alia, that the collaborative efforts must be based on a mutual exchange of information that is relevant to the parties’ respective areas of responsibility, and that the exchange of information is subject to provisions regarding the duty of confidentiality. All exchanges of information must be documented, and the relevant statutory provision must be identified. Requests for assistance in carrying out inspections may only take place within the respective administrative areas of the parties. In addition, procedures to which such requests are subject have been described in more detail. The procedure requires that requests must be made in writing, and that the statutory provision and legal basis for the inspection assistance, who is responsible for carrying out the inspection, and the administrative area that applies must be documented.

The fact that guidelines for the collaborative efforts between PST and customs authorities have now been developed, is highly significant, especially in terms of operational collaboration, where a clear framework for both the exchange of information and inspection assistance is vital. Customs authorities have wide discretionary powers to carry out inspections within their area of responsibility, whereas PST must obtain court orders authorising the search of property to carry out the same inspections. This means that there is potential for PST to circumvent these legal checks, and it is thus important to have a clear framework in place for collaboration between PST and customs authorities. These new guidelines contribute to this, in addition to facilitating for better external control on the part of the Committee.

9. The cooperation between PST and immigration authorities

The Committee has in recent years focused on increasing its knowledge of the collaboration between the EOS services and other public authorities, especially because more knowledge of these authorities will be relevant for the Committee's oversight activities. The Committee may also have a more direct responsibility of oversight of authorities that collaborate and exchange information with the services, cf. that the Committee's area of oversight is defined by function.

In its 2006 report, the Committee accounted for the cooperation between PST and the immigration authorities, and in 2007 the Committee met with Directorate of Immigration (UDI). In this meeting, UDI accounted for its cooperation with PST, among other things. The directorate stated that written guidelines for the exchange of information and contact between the service and UDI would be developed. The Committee has seen a draft of these guidelines, which are currently being considered by the Ministry of Justice. The Committee expects these guidelines to be implemented shortly.

In 2008, the Committee carried out spot checks of correspondence between PST and UDI in its inspections of PST. These spot checks did not reveal grounds for the Committee to initiate follow-up activities. In 2009 the Committee will continue its practice of carrying out spot checks of the cooperation between the service and UDI.

10. Investigation of PST sources/informants

In November 2008, the press revealed that an Afghan general living in Norway may have been involved in war crimes and violations of human rights. PST is rumoured to have cooperated with the general to get information about the situation in Afghanistan. The press claimed that Oslo Public Prosecutor's Office decided not to initiate an investigation of the general following a recommendation from PST, which allegedly argued that investigating the case would prove too difficult.

It is not within the scope of the Committee's mandate to evaluate the public prosecutor's decision not to initiate an investigation of the general. However, the Committee has the power to investigate the role of PST in this case, including the assessment on which a possible recommendation to the public prosecutor was based. In this regard, the Committee might deem it necessary to review the documents pertaining to the case, inter alia, to clarify whether the information shared with the public prosecutor is based on information on the general in PST's possession. Whether or not PST has made a deal with the individual to refrain from investigation in return for the individual's cooperation with the service or whether the service's recommendation to the public prosecutor is based on the notion that an investigation will impede the service's chances of gaining information from the source will be central to the Committee's investigation.

On the basis of the media attention, the Committee decided to investigate the case more closely. The investigations are still ongoing and will not be described further here. The case

raises some principal concerns regarding police use of sources/informants that may be guilty of serious crimes. The Committee will follow up on this specific matter in 2009 and return to the general problems associated with the use of sources/informants.

11. Preventive cases at a local PST unit

In inspecting a local PST unit, the Committee raised certain issues concerning three preventive cases. After the inspection, the cases were collected for closer review by the Committee. All three cases raised issues associated with annual re-evaluations and case progress, and in one case the Committee questioned the grounds for establishing the case. In addition, the Committee raised questions about the processing of personal data in a report.

Preventive cases may be established where there are "grounds to investigate whether individuals are planning a criminal act, and the prevention of which falls under the responsibility of the Police Security Service", cf. the guidelines for the processing of information in Section 3-5 of the PST Code of Practice. These guidelines further stipulate that the service, in determining whether or not to establish a preventive investigation, shall emphasise the current threat level, the nature of the information, including whether it is verifiable, and whether the scope of the preventive measures are proportional to the threat level. One of the investigations at this PST unit was established on the basis of a general concern related to the individual's physical appearance, social network, and alleged position in a religious community. There were no assessments found in the documents pertaining to the case that related to relevant penal provisions.

The Committee acknowledged that the threshold for initiating preventive investigations is low, and that decisions to initiate investigations are primarily based on the discretion of police experts. However, the Committee expressed that a certain concrete basis is required, and that information about religious convictions or physical appearance alone is not sufficient to justify initiating a preventive investigation. The Committee argued that the information relating to the individual's social network could possibly be sufficient, but that this information had not been specified in light of relevant penal provisions either. The Committee further noted that a high level of awareness is required in connection with initiating and processing information in preventive investigations in areas where there is a risk that processing data about an individual conflicts with Section 15 of the PST Code of Practice prohibiting the processing of data on an individual solely on the basis of religious convictions.

The Committee also had certain remarks in connection with updates and progress in three preventive investigations. In accordance with PST guidelines on the processing of data, preventive investigations must be kept up do date, so that they provide a comprehensive picture of relevant information, key topics for assessment, and the scope of the case. Furthermore, the documents pertaining to the case must demonstrate the progress of the case, and preventive investigations must be reviewed annually to determine whether or not there is grounds to carry the case forward. A review of the documents pertaining to the investigations showed a lack of progress, in that few, if any, investigative steps had been taken with the objective of confirming or repudiating whether the individuals were planning criminal acts that fall within PST's area of responsibility, despite the fact that the cases had been active for 3-4 years.

In its report to the Committee, the PST unit made reference to the DSE disposition circular, which states that preventive investigations must always be initiated when necessary, regardless of the capacity and expertise of the units. To this the Committee responded that the DSE guidelines are clear that cases must be kept up to date, and that all cases must show some progress. Even though the central administration of the service has permitted outstanding cases over some time, it is a clear premise that local units cannot allow

preventive investigations to remain open for years without any progress. The Committee thus was of the opinion that this situation ought to have been cleared with DSE. The Committee also pointed out that in re-evaluating the investigations no written reports had been developed as a basis on which to carry the investigations forward, and it was thus hard to ascertain whether there were in fact grounds to leave the case open.

The Committee also revealed grounds on which to criticise the PST unit for processing information in a report on all the identifiable individuals affiliated with a religious community, where certain individuals could be suspected of preparing criminal acts for which prevention is the responsibility of PST. The Committee revealed that the information had been processed in a local intelligence register, in conflict with DSE guidelines. In addition, the Committee found that the processing of personal data for some of the individuals conflicted with Section 15 of the PST Code of Practice prohibiting the processing of personal data solely on the basis of religious convictions. On this issue the Committee stated:

> "The Committee understands that investigations for preventive purposes require a somewhat wider scope initially, in order to map an environment. However, if an individual's affiliation with a religious community including people who are presumed to belong to an extremist environment is used to justify PST processing information about said individual, this is, in actual fact, a circumvention of the injunction on registering information solely on the basis of religious convictions. The Committee takes the provisions of Section 15 of the PST Code of Practice to mean that more specific information of relevance for PST is required about an individual in order to justify his or her registration. Furthermore, one must note that the justification for this provision in the guidelines is to protect all legal activities from PST registration. This provision requires that the service is aware of the distinction between legal religious activities, which does not give grounds for either the collection of information or the registration of personal data, and activities that give grounds for a specific suspicion that preparations for criminal acts are underway."

The PST unit has informed the Committee that the three preventive cases criticised by the Committee have been closed. As regards processing personal data about individuals affiliated with the religious community, the Committee has requested that a new evaluation be carried out as to whether the information should be retained by PST. The Committee will follow up on this matter in 2009.

IV. THE NATIONAL SECURITY AUTHORITY (NSM)

1. Inspections, general information about the supervision of the service

Inspection activities in the NSM follow a regular pattern. The Committee is provided with an account about ongoing activities in the service since the last inspection. In addition, an account is usually given about a specific topic, which is determined during the inspection preparations. At each inspection, and in accordance with Section 11, No 2 b of the EOS instructions, the Committee reviews all negative decisions made in connection with complaints since the previous inspection. Regular spot checks are also carried out on a number of negative security clearance decisions that have not been appealed, which the NSM obtains in advance from the clearance authority requested by the Committee. The Committee also inspects the service's electronic system for processing security clearance issues, as well as NSM records and archives.

In 2008, the Committee carried out four inspections of the NSM. Furthermore, the Committee inspected the personnel security clearance service of four clearance authorities: the Armed Forces' Security Section (FSA) (three inspections), the Norwegian Post and Telecommunications Authority, the Norwegian Petroleum Directorate, and the Police Security Service.

In 2008, the Committee received one complaint directed at the NSM. The Committee has expressed no criticism in the matter. In 2007, the Committee received two complaints in cases regarding security clearance determined by the Armed Forces' Security Section (FSA), and one complaint directed at the NSM. In one of the cases from 2007, specifically the one regarding FSA, the Committee expressed criticism. The case also raised the general issue of how to interpret the concept of enterprise in the Security Act and is described in more detail in Section 7.4 below.

On the basis of a concern expressed by the NSM in regards to the methods used by the FSA activities in the field of security intelligence, the Committee initiated an investigation of certain FSA cases. A key issue here is the methods legally available to the FSA in the collection of information regarding threats against the Armed Forces. The scope of the FSA's responsibilities in relation to other authorities, and the processing of obtained information were also addressed. The investigation highlighted several principal issues, which are described in more detail in Section 7.2 below.

2. Right to security clearance for relocating personnel in the Armed Forces

In its 2007 report, the Committee gave an account of a complaint concerning the need for security clearance among relocating personnel in the Armed Forces. This matter has been addressed in previous reports as well, in connection with the right to security clearance for information classified as Restricted in cases where security clearance has been revoked. In last year's report, the Committee requested, in its concluding remarks to the FSA on the matter, that the FSA initiate a speedy resolution to the general problem associated with security clearance for relocating personnel in the Armed Forces. The Committee further requested that the current clearance request for the complainant was processed without further delay, given that almost two years had passed since the complainant's observation period expired and he had not been offered another position. In connection with the specific evaluation of the complainant's case, the Committee noted that no justification could be found for granting security clearance for information classified as Confidential, but not for Secret, given that the evaluation was related to the need for security clearance. In its report, the Committee stated that it would follow up on further developments, both in terms of the general issue of security clearance for relocating personnel and of the complainant's specific case. In its remarks to the 2007 report, the Committee stated that it found it reprehensible that the case had not been satisfactorily resolved in 2007.

The Committee followed up on the case in 2008. In the spring of 2008, the complainant was granted security clearance for information classified as Secret. As regards the general issue of security clearance for personnel relocating within the Armed Forces, the FSA has informed the Committee that new procedures were implemented in May 2008 to deal with these types of cases, which means that requests for clearance by personnel under relocation will be processed. The Committee was informed that the procedures were temporary, due to the draft legislation for amendments to the Security Act, Section 19 of Proposition no. 21 to the Odelsting (2007-2008) relating to more stringent requirements for security clearance needs. The FSA noted that these amendments would require changes to the procedures of the Armed Forces and the Personnel Service of the Armed Forces (FPT) in personnel issues, so that individuals can be appointed to positions on the condition of being granted security clearance at a later date.

On the basis of the response from the FSA, the Committee gave the following remarks:

> "The Committee notes that the specific matter has been resolved and that the FSA has changed its procedures for processing security clearance requests for personnel in the Armed Forces currently under relocation. However, the Committee has some remarks to the temporary nature of these changes to the procedures, based on the drafted amendments to

Section 19 of the Security Act. One should note that these amendments have been approved, but have not yet taken effect.

As previously stated, these amendments entail more stringent requirements to the need for clearance, which is based on, inter alia, the assumption that the current requirements for security clearance needs result in an unnecessarily high number of clearance cases, which in turn may have negative consequences for relocating individuals. The Committee acknowledges the need to reduce the number of positions in the Armed Forces requiring a high security clearance. A reduction of this kind will probably also mean that relocating the personnel group involved in this case will become less problematic. However, the Committee does not see how these amendments are meant to entail a change in terms of the evaluation of clearance needs for personnel currently being relocated within the Armed Forces, given that the FPT indication of clearance levels in the Armed Forces in a letter to the Committee of 20 February 2008 is accurate as per today. Such an understanding would weaken the rights of the individual under the law, which was hardly the intention of the legislator.

In its concluding letter of 13 March 2008, the Committee stated that the FSA should be required to actively take part in finding a solution to the general issue of clearance needs for relocating personnel in the Armed Forces. The Committee noted that given the current situation, where superfluous personnel in the Armed Forces are prevented from completing a successful relocation for as long as they are without security clearance, the FSA should address this issue with the superior authority, and, if necessary, with the personnel authority. On this basis, the Committee presumes that the FSA will take the necessary initiatives to resolve the administration of this personnel group once the amended wording of Section 19 of the Security Act comes into effect.

The Committee requests to be informed of the FSA's further treatment of this issue."

3. Issues concerning the right to appeal decisions denying access to classified documents

In connection with a complaint concerning the revocation of security clearance, etc., the Committee has, in 2008 addressed certain general issues with the Ministry of Defence concerning the right to appeal decisions denying access to classified documents. As described in Section 3 of Chapter III above, specific procedures have been established in accordance with the regulations relating to information safety for petitions for access to classified documents. Section 2-13, Subsection 2 of the regulations states, inter alia, that the agency receiving the petition for access shall contact the issuing authority for an evaluation of the potential for declassification, and that the issuing authority shall report back whether the information may be declassified. The basis for this provision is that Section 2-11 of the regulations stipulates that classified information as a rule may only be reclassified by the authority issuing the information, said authority's superior authority, or the NSM.

Neither the Security Act nor the regulations relating to information safety contain provisions grants the right to independently appeal the decision of whether or not to reclassify the information, and the Committee thus assumed that the duty to assess the issue of classification, if applicable, would be based on an interpretation of the right to appeal pursuant to the statutory provisions on access in the appeal process as well, which in this specific case was the Freedom of Information Act. The Committee thus requested a statement from the Ministry on whether a duty exists to re-evaluate the declassification issue on the part of the appellate authority, when this appellate authority has the power to reclassify the information pursuant to Section 2-11 of the regulations relating to information safety. The Committee also requested the Ministry's view of whether the appellate authority, in petitions for access to documents transferred to the National Archives, is obligated to present the classification issue for the NSM or the agency superior to the document's issuing authority.

The Ministry of Defence sought the NSM's evaluation on this matter, which indicated that the issue of declassification is normally the determining factor in whether or not access is granted. The issue of declassification, however, is not subject to independent complaints, and the right to appeal decisions on declassification has no legal authority in either the Security Act or the regulations relating to information safety. Furthermore, the NSM stated that any obligation to consider classification issues in connection with petitions for access must be based on an interpretation of the provisions of Section 9 of the Freedom of Information Act and Chapter 2 D of the regulations relating to information safety, and that these provisions do not entail an immediate duty for the appellate authority to consider the issue of classification as well. The NSM further stated:

> "General administrative principles and actual considerations indicate, however, in our opinion that the issue of classification, too, will be evaluated by the appellate authority, provided that said authority has the power to do so in accordance with Section 2-11 of the regulations relating to information safety. Another interpretation will, in reality, render the dual-authority process a mere illusion in cases petitioning for access to classified information. This does not seem compatible with the principles on which the Freedom of Information Act is based. In cases where the appellate authority does not have the power to evaluate the issue of classification pursuant to Section 2-11 of the regulations relating to information safety, the NSM has, in a previous case, concluded that the issue of classification (but not the issue of access as such) must be presented for the NSM."

The NSM also carried out an evaluation of cases where the National Archives rejects a petition for access on the basis of insufficient declassification on the part of the issuing authority, and concluded that complaints in these cases would have to be processed by the administrative authority superior to the National Archives. The NSM further stated:

> "The procedure to follow in such cases is, as the NSM sees it, that the issuing authority is requested to evaluate the issue of declassification again. If the issuing authority upholds its original decision, the NSM believes, for the same reasons as mentioned under problem 1 above, that the issue of declassification should be reviewed by the administrative authority superior to the issuing authority, or, if applicable, the NSM."

Outside of the above, the Committee had no further comments and stated that the case had contributed to certain key clarifications in terms of how the provisions relating to the right to appeal decisions denying access to classified material should be interpreted. The Committee believes it is a matter of principle that individuals requesting access to classified material are granted the right to appeal decisions made in the first-instance authority. Given that the issue of declassification in most cases is the determining factor for whether or not access is granted, the view of the NSM, which is supported by the Ministry of Justice, will be highly significant for the individuals seeking access to classified material.

4. Inspection of the personnel security clearance service of the Ministry of Foreign Affairs

In its annual report for 2007, the Committee accounted for its inspections of the personnel security clearance service in the Ministry of Foreign Affairs. Following the inspection, the Committee had some comments to, inter alia, the authorisation procedures for the Ministry's own personnel and procedures concerning the lack of personal history data for closely related individuals in security clearance decisions. In its review of the 2007 report, the Standing Committee on Scrutiny and Constitutional Affairs asked the Committee to follow up on the matter. Following the Committee's concluding letter, the Ministry of Foreign Affairs has rebutted the Committee's criticisms in terms of interpreting Section 3-7 of the regulations relating to personnel security clearance.

It follows from provisions in Section 3-7 of the personnel security clearance regulations that information relevant for security issues is required for the last ten years for individuals that

form part of the personnel security clearance system. For security clearance at the level of Secret, this includes the spouse or life partner, in addition the person seeking security clearance. On the basis of an individual, comprehensive evaluation, security clearance may be granted pursuant to Section 3-7, Subsection 2 even if the 10-year requirement has not been met. In this regard, insufficient personal history data, due to, e.g. service on behalf of Norwegian authorities, may be emphasised in the evaluation.

The Ministry has stated that the accompanying family members of on expatriate assignments Norwegian authorities must also be covered by this exception in Section 3-7, Subsection 2, and that if the closely related individual's lack of personal history data is the result of him/her accompanying his/her spouse/partner abroad in connection with said individual's expatriate assignments for Norwegian authorities, the issue will not be further pursued in the security clearance process. Furthermore, the Ministry stated that the issue was addressed with the NSM.

The Committee stated the following to the Ministry on this issue:

> "In its letter to the Committee of 8 February 2008, the Ministry states that if the stays abroad by the closely related family member are the result of expatriate assignments for Norwegian authorities or accompanying family members in such assignments, "the stays abroad will not be subject to further evaluation". This is taken to mean that no specific evaluation of this issue will be carried out. One fundamental requirement of the Security Act is that each case must undergo individual evaluation, and the main element of the Committee's criticism of the Ministry's procedures in this area is how stays abroad seem to be generally dismissed even when they are the result of service on behalf of Norwegian authorities. Given that the equivalent stays abroad of the person in question seeking security clearance is likely to be treated the same way, one could envision cases where circumstances of great importance in a security clearance assessment undergo no individual evaluation whatsoever."

In terms of the Ministry's procedures for personnel security clearance, the Committee has been informed that the Ministry of Foreign Affairs is in dialogue with the NSM to establish an authorisation regime. The Committee will stay informed of any further developments on this issue.

5. Inspection of the personnel security clearance service in the Norwegian Post and Telecommunications Authority

In January 2008, the Committee inspected the personnel security clearance service in the Post and Telecommunications Authority. Following the inspection, the Committee raised issues relating to three of the clearance cases it had reviewed in random spot checks during the inspection in a letter to the authority. One of the cases concerned a lengthy process in dealing with a first-instance complaint, whereas the other two concerned issues of insufficient personal history data for spouses affiliated with other nations.

In its reply, the Post and Telecommunications Authority gave a detailed account of the time it takes to process administrative matters, both in terms of the specific case and on a general basis. As regards issues related to the lack of personal history data, the authority asked several follow-up questions related to the types of evaluations carried out by the authority in cases involving insufficient personal history data for spouses of individuals seeking security clearance.

In its reply, the Post and Telecommunications Authority further stated that the foreign national spouse in one of the cases had a personal history dating back one year, whereas for the spouse of the other case "it would appear that a history existed, dating back a little over two years at the time a decision regarding the issue of clearance was made".

In its concluding letter to the Post and Telecommunications Authority, the Committee stated the following:

> "*Time needed to complete administrative procedures*
> The Post and Telecommunications Authority admits that the time it has taken to complete administrative procedures in the specific case has been somewhat long. To explain, the authority makes reference to the need for obtaining additional information, as well as the decreased capacity of the authority due to the process of relocating from Oslo to Lillesand.
>
> The Committee has taken the authority's justification for the prolonged administrative process into account. However, the Committee still finds reason to point out that needing five months to reach a decision on a complaint is not satisfactory. Prolonged processes in matters concerning security clearance in business activities is irresponsible, both in terms of the specific case in question and in terms of the personnel administration with the requesting authority. The Committee understands that additional investigations in the field are sometimes necessary in connection with complaints. However, one would expect that part of the informational basis has been obtained previously, in connection with processing the clearance issue the first time around, and the Committee cannot see how additional investigations can justify the time spent on processing the complaint.
>
> *Insufficient personal history data for closely related individuals*
> Despite the fact that it is not clear from the documents pertaining to the case, the Post and Telecommunications Authority has stated that an evaluation has been carried out of the insufficient personal history data for closely related individuals in connection with assessments according to Section 21, Subsection 1, letters c and k of the Security Act. However, the authority has not provided a more detailed account of the evaluations it claims to have completed in the two specific cases.
>
> Pursuant to Section 21, Subsection 1, letter j of the Security Act, insufficient opportunities to carry out a satisfactory personal evaluation shall be a relevant aspect in an assessment of the individual's suitability for security clearance. Furthermore, it follows from Section 3-7, Subsection 1 of the personnel security clearance regulations that information relevant for security purposes must be present for the last ten years for individuals covered by the personal security clearance system. For security clearance at the Secret level this includes the individual's spouse or partner, in addition to the individual seeking clearance. On the basis of an individual, comprehensive evaluation, security clearance may be granted pursuant to Section 3-7, Subsection 2 even if the 10-year requirement has not been met. In this evaluation, the individual's affiliation with the country of origin and the significance of this country for the national security of Norway shall be emphasised.
>
> In that it is not clear from the documents of the case which evaluations have been carried out, and given that the Post and Telecommunications Authority in retrospect has been unable to account for this fact, the Committee has not been able to ascertain whether the decisions were based on a comprehensive, individual evaluation wherein the affiliation of closely related family members to […] and […], respectively, nor has the Committee been able to verify whether the security status of said countries has been assessed. It is the impression of the Committee that the authority may have been somewhat liberal in its assessment of the lack of personal history data in these specific cases. In this regard, the Committee remarks that the authority, based on the principle of fair and equal treatment, may want to clarify with the NSM which procedures the clearance authorities should apply in these cases.
>
> The Committee has also found grounds to point out that the Post and Telecommunications Authority has been unable to document that it has assessed the lack of personal history data on closely related family member in the specific cases. In one of the cases it is not even clear how far back the personal history went for the closely related family member before a decision was reached on the clearance issue. The provisions of the personnel safety clearance regulations stipulate a relatively specific assessment topic, which ought to have been documented in the internal concurrent justification. The Committee also notes that the evaluations carried out in accordance with Section 21, Subsection1, letters c and k are somewhat different than the evaluations carried out in accordance with Section 3-7 of the

personnel safety clearance regulations, and that the former cannot be presumed to include the specific evaluation required by the regulations. On the basis of information that the Post and Telecommunications Authority now has changed its administrative procedures, the matter will not be further pursued on the part of the Committee."

6. Inspection of the personnel security clearance service in the Norwegian Petroleum Directorate

In April 2008, the Committee inspected the personnel security clearance service in the Norwegian Petroleum Directorate. On the basis of what was revealed in the inspections, the Committee wrote the directorate and made certain general comments concerning the directorate's administrative procedures on security clearance issues, including a lack of internal, concurrent justifications in some cases, insufficient collection of additional information from the police, etc., and shortcomings in the procedures on archiving clearance cases.

In conclusion the Committee made the following remarks:

> "The circumstances highlighted by the Committee illustrate that the directorate's administrative procedures has had some shortcomings. The Committee believes that the low number of negative decisions may be one of the reasons behind not establishing satisfactory procedures in these respects. Decisions concerning security clearance may have relatively serious implications for the individuals involved, and the directorate must establish routines that safeguard the guarantees of due process of law built into the Security Act in the administrative procedures. On this basis, the directorate is asked to review and evaluate the issues highlighted here. The Committee requests that it be informed when this has been carried out."

In its response to the Committee, the Petroleum Directorate pointed out that some of the conditions emphasised by the Committee had been pointed out in the NSM inspection of the personnel security clearance service in the Petroleum Directorate in May 2007 as well. Furthermore, the directorate stated that it, under supervision of the NSM, had changed its routines for internal concurrent justifications, so that these now conformed to the requirements of the personnel security clearance regulations. The directorate had informed the NSM of this fact in a letter of October 2007. In addition, the directorate took the Committee's remarks into consideration. Following the account given by the Petroleum Directorate, the Committee did not deem it necessary to further investigate this matter.

7. Inspection of the activities in the Armed Forces' Security Section (FSA)

7.1 Introduction

Effective as of 1 January 2009, the Armed Forces' Security Section (FSA) changed its name to the Defence Security Service (FOST). The section was established in 2003, when the former Headquarters Defence Command Norway/Security Headquarters (FO/S) was abolished and its functions distributed between the NSM and the FSA. The recent name change was motivated by a greater correspondence with the function and role of the security service in the Armed Forces.

FSA is subject to the NSM's professional and supervising authority pursuant to Sections 8 and 9 of the Security Act in terms of the execution of preventive security services in accordance with the Security Act, including, inter alia, personnel security services. The Committee's oversight has previously been primarily geared towards the FSA as a security clearance authority. The FSA is the largest security clearance authority in Norway, and processed approximately 26,000 security clearance requests in 2008. The section processes security clearances for all military personnel, with the exception of security clearance for Intelligence Service personnel and security clearances at the top NATO level (CTS).

The inspection of the FSA as a security clearance authority entails being presented with all the negative clearance decisions made since the last inspection, in order for the Committee

to review these. In addition, the Committee inspects the archives and registers of the personnel security clearance department. The Committee also carries out random spot checks in accordance with clearly defined criteria. In 2008, the Committee questioned several clearance cases processed by the section. For more detailed information, cf. section 7.5.

In addition to inspecting the FSA as a clearance authority, the Committee was in 2008 informed of the activities of the FSA's operative security department. This department works to counteract security threats to the Armed Forces related to espionage, sabotage, and terrorist acts that may target the activities of the Armed Forces or threaten national security. The FSA has, on behalf of the Chief of Defence, been given the executive responsibility for this area.

The operative security department of the FSA has been given the overall responsibility for safeguarding critical security functions in the Armed Forces related to objects, personnel, materials, and information. In this regard, there is continual cooperation between the organised EOS services and the FSA. The activities of the operative security department of the FSA mirror the responsibilities of the organised services in civilian society. The FSA is different from the other services, however, in that it operates exclusively within the context of the Armed Forces and that the section does not have access to using invasive methods, such as electronic phone surveillance, room searches, etc. Investigations involving those types of methods must be carried out by PST or the regular police.

A key focal area for the Committee in inspecting the FSA is to make sure that the cooperation and exchange of information between the FSA and the organised EOS services takes place in accordance with the established frameworks and that the FSA does not operate within the areas of responsibility of these other services. As part of the Armed Forces, the FSA is familiar with the activities and security-related problems arising in this context. Measures and investigations associated with counter intelligence must be coordinated with PST, however, which is responsible for this field by virtue of being the domestic security service.

The Committee has been informed that a task force has been established within the Ministry of Defence to explore the areas in which the EOS services and the FSA intersect, assessing whether there is a need for further clarification. In 2009, the Committee will keep informed of these activities.

7.2 FSA's methods within the field of security intelligence

In 2008, the Committee reviewed three cases processed by the FSA's operative security department. The Committee first learned of these cases in a meeting with the NSM, which, on the basis of, inter alia, information it had received, expressed concern about the sections methods in a letter to the Ministry of Defence. The nature of the conditions described by the NSM indicated that an investigation ought to be launched, safeguarding faith in independence and objectivity. On questions of how the matter was being addressed, the Ministry of Defence responded that it had not commenced any organised investigation of the matters, but that the Ministry had requested a written statement from the Chief of Defence as a basis on which to assess the need for further investigation. In this situation, the Committee deemed it expedient to deal with the matter on its own, without awaiting the results of any investigations launched by the Ministry. The Ministry was informed of this fact.

The investigation has included reviewing documents and interviewing FSA personnel, as well as other individuals that are familiar with these cases. As part of the investigation, the Committee has also obtained general information about the cooperation between the organised services and the FSA. The investigation into the matter has been substantial up to

this point, and because the investigation is still ongoing the cases will not be described in more detail here. However, already at this point the Committee feels confident in stating that there are some uncertainties relating to the role and mandate of the FSA, as well as to the methods legally available to the FSA in gathering information about threats to the Armed Forces, both domestically and abroad.

In security legislation, the FSA is given the responsibility to investigate the circumstances surrounding events threatening the security of the Armed Forces, and to implement measures aimed at reducing the potential consequences. Events threatening security have been defined as activities threatening security, i.e. espionage, sabotage and acts of terrorism, compromising classified information, and serious breaches of security. In order to uphold this responsibility the FSA must be able to obtain information about events threatening security. However, the regulations do not specify how, or by what means, this information is to be obtained.

Without legal authorisation the FSA will not be able to use invasive measures towards Norwegian citizens, nor will it be able to do so against military personnel, in Norway or abroad. However, the methods available without such expressed authority must be specified in detail. In cooperating with other authorities one must look to the legal basis of the cooperating authority. Even when the objective is to safeguard the Armed Forces from threatening activities, a certain level of awareness concerning legal basis is essential. When investigations target individuals the consideration of safeguarding the Armed Forces must be balanced against the rights of the individual to protection under the law.

The uncertainties of the regulatory situation of the FSA are highly unsatisfactory. The FSA has been given key responsibilities in the Armed Forces, and the framework for its activities must thus be subject to a greater degree of regulation. Since the establishment of the FSA in 2003, the section has received substantial funding to uphold its responsibilities. When the ongoing investigations are concluded, the Committee will address the uncertainties of the regulatory situation with the FSA and the Ministry of Defence. This matter will be addressed in more detail in the 2009 annual report.

7.3 Right of access when a security clearance case is dropped

In its 2007 report, the Committee described a complaint of the FSA's handling of a petition for access in a security clearance case. The complainant had petitioned for access to a clearance case, which had been closed because the need for clearance had lapsed. The complainant's petition was denied, as the FSA did not deem its decision to close the case warranted a right to access pursuant to Section 25a of the Security Act. A later complaint of the refusal to grant access was rejected by the FSA on the same grounds.

Section 25a of the Security Act stipulates that the right of access applies once "the decision on security clearance" has been made. In a letter to the FSA, the Committee writes that both the preparatory works of the Act and actual considerations indicates that closing the case should be regarded as a security clearance decision. The Committee made reference to the fact that closing a case may encompass many different types of situations where access rights may be present. On this basis, one could hardly regard it as obvious that no rights of appeal were present pursuant to the Security Act, as indicated by the FSA. However, the Committee did not reach a decision on this matter, but presented it to the NSM on a general basis.

The Committee has followed up on this matter in 2008 and has requested that the NSM evaluate the general issues raised by this case. In its response to the Committee, the NSM accounted for its procedures for closing cases and provided an evaluation as to whether rights of access and rights of appeal apply to closing decisions. The NSM made reference to

how Section 3, no. 16 of the Security Act defines security clearance as a decision made by the issuing authority on the basis of a personal evaluation about an individual's presumed security suitability for the specified security clearance level. As regards the issue of whether closing a case constitutes a "security clearance decision" to which rights of access applies, the NSM stated:

> "The NSM agrees with the Committee that the wording of the provision indicates that the legislator has imagine a positive or negative decision (an actual decision) being made before the rights of access come to apply. The preparatory works give, as the Committee pointed out, no indications as to the meaning outside of the wording itself. The Committee points out that general considerations favouring rights of access should apply equally, even if a case is closed. The NSM does not accept the view of the Committee in this regard. In the NSM's view, closing the case does not automatically invoke rights of appeal for the individual in question, cf. the above account. In our view, gaining access to the documents of the case would weaken the individual's legal standing. The regulatory context further indicates that rights of appeal should not be inferred when cases are closed.
>
> Furthermore, the NSM believes that rights of access to closed cases can be problematic in some instances. The justification for only granting rights of access *after* a decision has been made can be found in security-related concerns. These apply to some closed cases as well, where the individual reapplies for clearance within a certain period of time after the case was closed. In these cases, the information from the closed case could form part of the new clearance case, in accordance with Section 4-8, Subsection 2 of the regulations relating to personnel security.
>
> ---
>
> If the individual is granted access to the information possessed by clearance authorities prior to the authority making a decision, the individual will, inter alia, be able to adjust his assessments and statement in security interviews, for example. These adjustments will make it very difficult for the clearance authorities to form a real opinion of the individual's reliability, loyalty, and good judgment. Consequently, this could prevent the case from establishing a sufficient or truthful basis of information, which must be deemed to represent a security problem. In terms of closed cases, considerations of this nature will be relevant in cases where an individual might reapply for clearance within a set period of time. In general, the same information will form the basis for decisions in both cases, and the individual could then be granted access to the new case if this results in an actual decision."

Following this, the NSM concluded that the Security Act, with pertaining regulations, does not contain stipulations indicating that a closed case may be regarded as a security clearance decision, and that neither the preparatory works nor actual considerations indicate a wider interpretation of a relatively straightforward legal text. In light of this, the NSM concluded that a closed case could not generate claims for a written notification including the basis on which the decision was made, rights of appeal, or rights of access.

In a letter to the NSM, the Committee made the following remarks:

> "This case raises the issue of the nature of a decision to "close" a security clearance case, including the issue of whether a decision to close a case must be regarded as being covered by the wording of, inter alia, Section 25 of the Security Act, which refers to "decisions on security clearance". The Committee initially notes that regardless of how one characterises the closing of a case, it naturally follows that a decision has been made by an administrative authority, which in turn entails that general administrative provisions do apply.
>
> Pursuant to Section 25a, 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 "[o]nce a decision on security clearance has been made". Rights of access to one's own case must be regarded as an established administrative

principle and is a fundamental prerequisite for the possibilities of the individual to safeguard his standing.

As described above, the wording of the provision in question may indicate that the legislator envisions either a positive or negative actual decision being made before granting rights of access, which is further substantiated by the legal definition found in Section 3 of the Security Act. However, the preparatory works offer no indication that various situations in which the administrative procedure is concluded prior to making any actual decision were considered at the time the legislation was drafted. The Committee thus maintains that the wording of the legal definition of Section 3 and the provisions of Section 25a offer limited instructions in terms of the specific category of decision in question here. In such cases, one must take into account actual considerations and general administrative principles.

The NSM has pointed out that rights of access to closed cases in some cases may be problematic, especially in cases where the individual reapplies for security clearance within a certain time period after the initial case being closed, because the individual then is able to position himself in relation the information possessed by the clearance authority. The Committee can understand this view, especially in cases where the individual is the subject of several clearance cases during the same timeframe. However, if some time passes before the individual in question reapplies for clearance, the case is not deemed to be any different from a case involving a negative clearance decision, where the individual is free to reapply once the observation period has expired. In any circumstance, the Committee cannot see why security considerations that apply to a small number of cases only should cut individuals off from the fundamental right to access information pertaining to one's own person.

The preparatory works of the Act give no indication that the legislator's intention has been to exempt decisions to close cases from rights of access under Section 25a of the Security Act. The provisions in question regulate party rights. In that it has been established that the party's rights of access are equally applicable when a case is closed as in cases involving an actual decision, and that the legislator did not intend to make exceptions, this is indicative of a strict interpretation, true to the wording of the provision. The Committee thus concludes that the wording of Section 25a of the Security Act must be interpreted more widely, entailing that a "decision on security clearance" is interpreted as including a decision to close a security clearance case as well. Whenever specific security concerns are present, one must of course allow for exemptions to the rights of access, preferably in the form of an extension, cf. the above discussion."

The Committee has requested that the NSM carry out a new evaluation of the general issues raised by this matter.

7.4 FSA's administrative procedures on dealing with complaints – the concept of enterprise

The Committee investigated a complaint concerning the FSA's administrative procedures relating to security clearance and authorisation. The Security Act stipulates that access to information classified as Confidential or higher requires security clearance and subsequent authorisation, whereas for the lowest level of classification, Restricted, only authorisation is required. The complainant, who was employed by the Armed Forces, needed authorisation to access Restricted information in this position. However, as he did not have access to information classified as Confidential or above, security clearance was not required.

In the complainant's case, the FSA had received information about an ongoing investigation of him. In light of this negative information, the FSA wrote letters to the complainant and his employer, respectively, informing them of why the complainant was not granted security clearance. In its letter to the complainant's employer, the FSA also ordered the person granting authorisations to refrain from authorising the complainant. The FSA has informed the Committee that these letters were intended as information about the complainants clearance status, but that it, in retrospect, acknowledged that the letters had a wording/construction fit to generate misunderstanding. The Committee criticised the FSA for this, and pointed out that it seemed as if the FSA's actions in this matter were used as part of

the justification for discharging the complainant, who was discharged in connection with the investigation.

The case also raised the general issue as to the role the FSA plays in cases involving authorisation for personnel in the Armed Forces. The Committee presumed that the uncertainty in the complainant's case was based on the interpretation of the concept of enterprise as it is applied in the Security Act. This concept is in the Security Act defined as "an administrative body or other legal person subject to the provisions of the Act", cf. Section 3, Item 6. The concept is central to the security legislation and plays a vital role in, inter alia, the responsibilities and duties of the preventive security services. However, the specifics of this concept have not been established in terms of the various units of the Armed Forces. The Committee believes this matter illustrates the uncertainties that may arise in individual cases and requested that the Ministry of Defence evaluate the concept of enterprise. The Committee will follow up on this issue in 2009 and return with a more detailed account in its next report.

7.5 Individual cases discussed with the FSA

Over the course of 2008 the Committee has raised issues relating to several individual cases involving security clearance with the FSA, in light of random spot checks among negative clearance decisions made by the section. This type of oversight activity has been implemented as a standard routine during Committee inspection of the FSA.

In one case, the Committee questioned the section's revocation of a security clearance where the justification for the revocation was a matter that was known already at the time the individual was granted clearance. After addressing issues related to the access to overturn the revocation decision, the Committee requested that the FSA consider the case again. The Committee asked to be informed of the FSA's final decision in the case. At present, the Committee has not received any information about this case from the FSA and thus presumes that the matter is still being considered.

In another case, the Committee raised questions about the FSA threshold for carrying out security interviews in cases where the personal evaluation revealed that the individual had been in contact with drugs. On this matter, the Committee concluded as follows:

> "Pursuant to Section 21, Subsection 3, third sentence of the Security Act, a security interview must be carried out in cases where such an interview is deemed "clearly unnecessary." The purpose of a security interview is to contribute to a satisfactory mapping of the individual's security qualifications and to facilitate for an individual evaluation of the case. This provision also stipulates requirements for the rights of the individual to protection under the law.
>
> The Committee has taken the FSA's statement that it for resource purposes has adopted a somewhat restrictive practice in assessing when a security interview is required into account. The Committee cannot see that this type of consideration is relevant pursuant to the provisions of Section 21 of the Security Act, which stipulates that the clearance authority must carry out security interviews in cases involving an element of doubt. A restrictive practice in the use of security interviews in the FSA for practical purposes may entail that the personnel of the Armed Forces are subjected to a more stringent assessment than personnel in the civilian sector in terms of when security interviews are carried out. This could be problematic in relation to the principle of fair and equal treatment.
>
> Furthermore, the Committee finds the practice where the FSA relies on phone interviews in an ever-increasing number of cases, perhaps even replacing the security interview, to be problematic. The Security Act, with pertaining regulations, stipulates a number of requirements that apply to the security interviews. For example, the individual interviewed has the right to have assisting counsel present for personal support. The Instructions to Chapter 6 of the Security Act and the regulations relating to personnel security established by the NSM under and pursuant to Section 26, Subsection 2 of the Security Act further describe the security

interviews and how they are to be executed, cf. Item 3.4.2. It follows from the instructions that a security interview should be planned and executed in such a manner that the purpose – determining the individual's suitability for security clearance – can be fulfilled. Furthermore, the provisions stipulate that the interview should be carried out in an undisturbed atmosphere facilitating the necessary level of good faith.

A phone conversation would normally not fulfil these requirements. However, in its letter the FSA points out that the phone conversation is only intended as a supplement to a regular security interview "in cases where there is still some lingering doubt". The Committee takes this statement to mean that the FSA in cases involving doubt will call the individual initially, but that a security interview will be carried out if the phone call does not eliminate the doubt. If this is the case, an individual may talk his way into an "unclassified" as well as into a positive security clearance. In the Committee's view, this practice conflicts with the "must"-provision of Section 21 of the Security Act. Measures aiming to reduce processing time must not be implemented to the detriment of the rights of the individual to protection under the law."

Following the Committee's concluding letter on this matter, the FSA has informed the Committee that the section has reviewed its routines for using phone calls in matters concerning personnel security.

7.6 Case processing time in cases concerning security clearance

In its two previous annual reports, the Committee has commented on the FSA's case processing time in cases concerning security clearance. In its 2007 report, the Committee explained that the situation had improved dramatically, as a consequence of the personnel situation improving and a project aiming to reduce the backlog of older, outstanding cases. The Committee noted that steps had been taken to reduce the processing time, but still had not reached acceptable levels. The Committee presumes that the activities in this regard remain high on the list of priorities, and that the Committee will be kept informed of developments on the matter.

In its inspections at the FSA in 2008, the Committee requested to be informed of the status of case processing times in clearance cases. The section further accounted for other challenges associated with the processing of clearance cases, inter alia in connection with archiving, mailing procedures, and the electronic processing application for clearance cases (TUSS).

The backlog of personal evaluations was, according to the FSA, gradually reduced over the course of 2008, and at the end of the year the section had no such backlog left. Backlogs of clearance case decisions have been reduced by half in 2008, despite the fact that 2008 saw more requests for clearance than 2007. Furthermore, separate routines for the FSA's processing of clearance cases were developed, as well as guidelines for the processing of various types of cases, such as cases involving findings associated with drug use or financial situations.

The objective of the FSA for 2009 is to process clearance cases within six weeks on average, but the section recognises that some types of cases will take longer, for example if there is a need to obtain additional information through personal evaluations. The section has informed the Committee that all cases must be processed within one year, regardless of complications. Furthermore, the section is working to fill all the available positions in the personnel security department, which has been understaffed and characterised by heavy rotations in recent years. The section will continue to emphasise improving the expertise of its executive officers and increasing the quality of the administrative procedures. Also, the FSA will carry out security interviews in more cases than previously. In cases where the personal evaluation does not reveal any registrations in various registers, the FSA aims to reach a conclusion within two to three weeks. The FSA has informed the Committee that it

cooperates closely with the NSM in terms of implementing various measures to reduce the case processing time in security clearance cases.

In light of the Committee's comments to the case processing time in security clearance cases in the 2006 annual report, the Ministry established a task force in the fall of 2007. This task force comprised representatives from the Ministry of Defence, the NSM, the FSA, and the National Service Administration. The efforts of the task force resulted in a report, recommending specific measures aimed at reducing processing times in security clearance matters involving personnel called up for initial service. In its report, the task force pointed out that the total number of security clearances in the Armed Forces is too high in relation to actual security needs. Furthermore, the task force questioned the clearance levels of conscripts. The task force suggested, inter alia, that the Armed Forces review the types of positions requiring security clearance, increased emphasis on other forms of precautionary measures over personnel security clearance (such as physical safeguards), better reporting routines for personnel with security clearance, and improved electronic processing routines.

The FSA's comments to the improvements in case processing time for security clearance cases emphasise that the section is still actively working to reduce backlog, and that these efforts have yielded great results. Consequently, the Committee did not deem it necessary to initiate further follow-up activities in terms of the FSA case processing time other than staying informed of developments. The Committee will continue to stay informed of developments in 2009 as well.

V. THE INTELLIGENCE SERVICE

1. Inspections, general information about the oversight of the service

In 2008, the Committee carried out three inspections at the Intelligence Service Headquarters. Furthermore, the Intelligence Service units at the Joint Operative Headquarters (FOHK) and the Regional Command in Northern Norway (LDKN) were inspected, as well as the F/S Marjata.

The Committee investigated one complaint against the Intelligence Service in 2008. The Committee has not expressed any criticism on the matter.

In 2008, the Committee has, in light of one specific case, raised various issues with the Intelligence Service concerning the interpretation of Section 4 of the Intelligence Service Act, which stipulates that the Intelligence Service "shall not on Norwegian territory monitor or in any other concealed manner procure information concerning Norwegian physical or legal persons". In this case, the Committee raised the issue of whether Section 4 should also apply to requests for information from the Intelligence Service to PST. The matter contributed to establishing certain key clarifications and is further described in Section 2.

In its 2007 report, the Committee focused on the increased cooperation between the Intelligence Service and PST and how access to this collaboration is a prerequisite for being able to complete relevant and comprehensive oversight. The Committee also gave an account of its investigations into a joint operation between the Intelligence Service and PST and the legal basis for the Intelligence Service's role in the operation. This matter is addressed in more detail in Section 3 below.

2. Request for information from the Intelligence Service to PST

In light of a request within the field of counter intelligence from the Intelligence Service to PST regarding a Norwegian citizen, the Committee addressed issues concerning the interpretation of the ban on the surveilllance of Norwegian citizens stipulated in Section 4, Subsection 1 of the Intelligence Service Act in a letter.

In its reply, the Intelligence Service accounted for the background on which the request to PST was made and argued that the analyses and assessment behind this request were well within the responsibilities of the service. The service gave an account of the response it received from PST and noted that it was not aware of whether the individual was a Norwegian citizen at the time it submitted the request to PST. The Intelligence Service deemed that the request was not in conflict with stipulations contained in Section 4 of the Intelligence Service Act.

Furthermore, the service discussed, on a general basis, whether a request from the Intelligence Service to PST regarding information about Norwegian citizens entailed obtaining information in "any other concealed manner", but upon reviewing statements in the preparatory works regarding foreign intelligence enterprises and the purpose of the Intelligence Service Act, as well as actual considerations, it found that this was not the case.

In light of the reply from the Intelligence Service, the Committee commented that it took the service's letter to mean that no final conclusion had been drawn on the issue of whether obtaining information from PST could be considered concealed collection of information, but that the service had concluded that Section 4 of the Intelligence Service Act allowed for the collection information in this manner in special cases. The Committee pointed out that certain critical considerations in some cases indicated that the service should obtain information from PST, even on Norwegian citizens in this country, particularly in areas in which the responsibilities of the services overlap. The Committee commented that the interpretation and application of Section 4, Subsection 1 of the Intelligence Service Act should be clarified with the Ministry of Defence, which has the administrative authority for this Act. The Committee thus requested that the service present the matter to the Ministry for review.

The Committee did not draw any final conclusions on the issue of whether the service's interpretation of the act was legally viable, but the Committee still commented that it, on a general basis, was hard to argue that certainty as to the citizenship of an individual would be decisive, and stated that a certain level of caution was in order, given that the service was informed of the individual's home address. Furthermore, the Committee commented that the service ought to have completed the evaluation carried out once the Committee took issue with the case ahead of time and not after the fact.

In its reply, the Ministry of Defence initially pointed out that the general problem was limited to whether the Intelligence Service should have access to obtaining information from PST on Norwegian citizens in Norway, and that the general prerequisite for any legal basis in this matter is that the Intelligence Service, through this exchange of information, seeks to obtain information that falls within the purposes of the Act and the responsibilities of the service. Furthermore, the Ministry emphasised that any action taken must concern the collection of information about Norwegian citizens fit to shed light on foreign affairs, and that any future requests to PST should be clearer on the basis on which these requests are made, as well as the type of information the service seeks to obtain.

On the issues of interpretation associated with this matter, the Ministry stated:

> "In the main, the Ministry of Defence agrees with the general view of the Intelligence Service regarding the interpretation of Section 4, Subsection 1 of the Intelligence Service Act, which is explained in the service's letter to the EOS Committee of 20 February 2008. Hereunder, we agree with the view of the service that one must distinguish between the self-collection of information (concealed intelligence operations on Norwegian soil against Norwegian citizens, which is what Section 4, Subsection 1 of the Intelligence Service Act primarily intended to ban) and the exchange of information concerning Norwegian citizens from PST to the service. In

the latter case, this distinction between domestic intelligence and foreign intelligence is upheld.

The Ministry of Defence is thus inclined to argue that a pure exchange of information between the two services is unlikely to be regarded as “a collection of information” in the legal sense of the term, because both the connection between the concept of “surveillance” and actual considerations indicate that the concept of collection presupposes a certain level of active participation on the part of the service outside of submitting an RFI [Request for Information] to PST. If PST, of its own volition, transfers such information to the Intelligence Service, one could hardly conclude that this involves data collection on the part of the Intelligence Service.

In any event, and even if one were to conclude that this exchange of information is covered by the concept of collection as applied in Section 4, Subsection 1 of the Intelligence Service Act, one could raise the issue of whether the retrieval of information is “concealed”. The Intelligence Service will in many cases not know the manner in which PST has come to possess the requested information, or the information that ex officio is transferred from PST to the Intelligence Service. And even if the Intelligence Service was made aware that PST has obtained this information through the use of concealed measures, it is not necessarily the case that the *dispatch of information* is concealed, in the sense of Section 4, Subsection 1 of the Intelligence Service Act. The fact that the two services exchange legally obtained information relating to, inter alia, international terrorism, should be widely known and is established in publicly available instructions, etc. Thus, we cannot see how Norwegian citizens can legitimately expect PST not to convey information about them to the Intelligence Service, provided that the purpose of the conveyance is to maintain a flow of information concerning the activities and connections of Norwegian citizens directed at foreign nations and foreign affairs.”

Following this, the Ministry evaluated the actual concerns present and made reference to the cooperation instructions between the Intelligence Service and PST, which presupposes an exchange of information between the services. The Ministry concluded requesting information from PST concerning Norwegian citizens in Norway in certain areas is not subject to the ban of Section 4, Subsection 1 of the Intelligence Service Act.

In closing, the Committee contributed the following comments to the Intelligence Service:

“The matter raises some principal questions regarding the interpretation of Section 4, Subsection 1 of the Intelligence Service Act, which prohibits the service from “monitoring or in any other concealed manner procure information” concerning physical or legal persons in Norway. The Committee takes the Ministry’s account to mean that in the interpretation of Section 4, a distinction must be made between self-procurement (concealed intelligence operations on Norwegian soil against Norwegian citizens) and the exchange of information concerning Norwegian citizens from PST to the Intelligence Service.

The Committee regards this distinction between operative activities and the exchange of information to be essential in the interpretation of the ban stipulated in Section 4. In light of the Ministry’s account, wherein this distinction is emphasised, the Committee has no further questions. However, there is reason to emphasise the importance of not being too restrictive in interpreting the scope of the ban. In this context, reference is made to a letter from the Committee, dated 4 July 2008, wherein it states:

> “On the other hand, Section 4 of the Intelligence Service Act is a provision intended to protect Norwegian citizens in this country from Intelligence Service activities, both in terms of its wording and in terms of its preparatory works, cf. the letter from the Ministry to the Standing Committee on Defence, dated 18 November 1997, Item 2, among others. This provision is thus essential both because it safeguards the rights of the individual to protection under the law and because it represents the demarcation between the areas of responsibility of the Intelligence Service and PST, respectively. The nature and function of the provision, in the view of the Committee, are indication that one should not apply restrictive interpretations as to the scope of the provision, as

this is expressed in the Act, including further substantiation in actual considerations and statements included in the preparatory works of the Act. Furthermore, one can hardly take the preparatory works of the Act to be indicative of a restrictive interpretation of this matter. Statements in Proposition no. 50 to the Odelsting (1996-97), Chapter 9, regarding how the service must be able to procure information about foreign intelligence and other foreign activities, is, as far as the Committee can tell, justified in the service's needs to protect itself – its own installations and capacity – i.e. against activities directly targeting the service. Furthermore, this is the only field in which the Intelligence Service instructions, in Section 5, Subsection 3, allows for a certain level of active participation on the part of the service in procuring information. A similar interpretation may also be found in the Ministry of Defence's letter to the Standing Committee on Defence, dated 18 November 1997, wherein the Ministry, inter alia, states:

> "A certain level of active and concealed procurement of information in this regard may, however, still be necessary in order to gain full insight into threats, thereby safeguarding the installations of the Armed Forces against foreign intelligence activities."

In this context, one might want to interpret both the preparatory work and the instruction in a manner, which establishes a clear and present need to keep the service informed. It does not naturally follow, however, that this is mirrored by the service's operative activities in general."

In the Committee's opinion there are no grounds on which to criticise the specific request made in this case. This is primarily justified by the exchange of information between PST and the Intelligence Service not being regarded as "monitoring or in any other concealed manner procuring information", and the exchange of information taking place in this case fell within the statutory responsibilities of the Intelligence Service. In addition, the Committee has taken note of the Ministry's emphasis of how future RFIs to PST should include information about the background for the request and the types of information sought by the service. Furthermore, this would facilitate for better external oversight on the part of the Committee in this area."

The clarifications yielded by this case serve as points of departure for the Committee in its future oversight activities, checking to see that the service does not infringe on the ban against surveillance of Norwegian citizens. The Committee will continue to emphasise these aspects in its inspections of the Intelligence Service.

3. Joint operation between PST and the Intelligence Service

As described in Chapter III, Section 7 above, 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.

The Committee asked the service to account for how they evaluated their actions vis-à-vis the provisions of Section 4 of the Intelligence Service Act, as well as for how this case had been handled in relation to the procedures the service has implemented for the political approval of methods and operations. Furthermore, the service was asked to give a detailed account of the purpose of the operation.

The service gave said account of the contents of the operation, informed the Committee that the contents of the operation had been evaluated and found 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 Intelligence Service. Furthermore, the service stated that the operation was directed at activities abroad and that the targets of the operation were not Norwegian citizens.

In its evaluation, the Committee made reference to statements contained in the preparatory works on Section 4 of the Intelligence Service Act, which expressly prohibits the Intelligence Service from engaging in concealed intelligence activities directed at Norwegian citizens in this country. The service was requested to review the legal basis for the measures in question again. This aspect of the case is still pending.

4. Political approval of methods and operations

In previous reports, the Committee has commented on the scope of the Intelligence Service Act as an independent legislative framework for the use of invasive methods and its significance for legality, in that methods used have been evaluated and approved by the responsible public authorities. In this case, the Ministry of Defence has stated that political approval of new methods and special intelligence operations is essential, and that failing to obtain approval under the circumstances of each case can have consequences for the issue of whether the use of a method can be considered lawful. The Ministry has furthermore expressed that political approval of methods and operations must be formalised in writing, so that said approval is recoverable within the service and verifiable for the EOS Committee.

As described by the Committee in its 2007 report, the Ministry has raised certain issues regarding the Committee's access to ministerial evaluations forming the basis for an approval. In its concluding letter to the Ministry on this matter, the Committee stated the following:

> "The Committee is satisfied that the Ministry now has established procedures for the processing of matters presented to the Ministry pursuant to Section 13 of the Intelligence instructions. If the procedures have been laid down in an instruction or other formalised instrument within the Ministry, the Committee would like to receive a copy. If this is not the case, the Committee will relate to the description contained in the letter to the Committee.
>
> As far as the Committee is aware, the Committee and the Ministry are now largely in agreement about the issues raised concerning access to the approval process for cases involving Section 13 of the intelligence instructions. However, there may still be grounds to summarise the views of the Committee, and a natural point of departure will be the monitory needs of the Committee in this area.
>
> The practice of the Intelligence Service seeking the Ministry's approval prior to adopting new methods for data collection and prior to implementing special intelligence operations is firmly established. The purpose of this arrangement is perhaps primarily to secure political support for and accountability of activities that may affect other states. However, the Committee presumes securing political support may be important in other contexts as well, especially if the activities include the use of invasive methods in areas where no legal basis for their use exists (or where this legal basis may be unclear).
>
> Developments in recent years have meant that international human rights, as well as national principles of the rights of individuals to protection under the law, have been operationalised to a greater extent than previously. Consequently, in evaluating the legality of methods and operations today, authorities will have to include such principles and rules of law in their assessments.
>
> Overseeing the legality of the activities of the services is part of the Committee's statutory oversight duties. The Committee must place particular emphasis on the rights of the individual to protection under the law, cf. Section 2 of the Act relating to the Monitoring of Intelligence, Surveillance and Security Services. On this basis, the Committee deems it especially important to inspect whether a case has been presented to the Ministry, the information that was provided in each case, the legal issues raised by the service, if applicable, and the contents of the Ministry's decision.
>
> If the Ministry does not find it expedient to establish an arrangement where Section 13 cases must routinely include, in a form to which the Committee can gain access (preferably within

the service), statements as to which legal issues, if applicable, were brought before the Ministry, the Committee will not pursue this issue further. It is possible that such an arrangement may be regarded as principally suspect in relation to the Ministry's wish to safeguard internal assessments. The Committee does not have access to the internal documents of the Ministry and will, of course, fully respect this. However, an arrangement as described above could reduce the amount of paperwork exchanged between the Committee and the Ministry in individual cases. The current practice is that the Committee, in cases where the Committee's oversight responsibilities require further investigation, first approach the service with questions. If this does not prove sufficient, the Committee must then address the matter with the Ministry in writing.

In conclusion, the Committee would like to comment on the Ministry's statements concerning Section 6 of the Act relating to the Monitoring of Intelligence, Surveillance and Security Services and the Committee's area of oversight. Provisions in Section 6 of the Act limit the Committee's right of access to the ministries and the obligations of ministry personnel to give evidence, etc. These provisions are based on constitutional concerns, but they are not to be interpreted in such a manner that the ministries are exempt from the Committee's area of oversight, which is functionally defined in Section 1, Subsection 1 of the Act. The fact that ministry personnel shall not be exempt from oversight is evident from, inter alia, Section 10 of the monitoring instructions. In addition, reference is made to the recommendations of the Skauge Committee (NOU 1994:4), Chapter 4.5.5. The Committee must exercise caution in its oversight activities involving the ministries, cf. Proposition no. 83 to the Odelsting (1993-94), p. 22, 2nd column, and the Committee believes it has exercised such caution in its activities."

In a letter to the Committee, the Ministry confirmed that the understanding of the Committee corresponds well with established Ministry routines. In 2008, the Committee has also been presented with cases in the Intelligence Service that have been approved by the Ministry. The Committee has not found grounds to comment on the approval procedures currently in place.

5. Exchanging information with foreign collaborative services

In its report for last year, the Committee described the establishment of a inspection routine for the exchange of information between the Intelligence Service and foreign collaborative services. This inspection primarily concerns one of the larger communication systems within the field of counter terrorism and is organised in such a way that the Committee can access the communication system, conducting searches and random spot checks among the messages sent by the service. The service will assess, ahead of time, whether it needs to make exceptions to the Committee's access in order to protect its sources, and 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.

The Committee has in 2008 inspected the communication systems of the service. Under and pursuant to Section 4 of the Intelligence Service Act, the Intelligence Service may not, on Norwegian soil, procure information about Norwegian physical or legal persons. In terms of the Committee's oversight responsibility, the main issue is ascertaining whether the service upholds the injunction on surveillance of Norwegian citizens, and how information or requests for information pertaining to Norwegian citizens are handled.

The service adheres to the established practice that information about Norwegian citizens received by collaborative partners will normally either be deleted or transferred to PST if it is deemed to be of interest to them. Information forwarded to PST is logged by the Intelligence Service and is accessible to the Committee. The service does not disclose information about Norwegian citizens to foreign collaborative partner, not even in the international counter terrorism collaboration.

Committee inspections of the exchange of information with collaborative services have in 2008 not revealed grounds for criticism.

6. The Committee's inspection of the service's technical information procurement

In 2008, too, the Committee was continually informed of the service's efforts to develop its capacity and methodology for technical information procurement. The processing and analysis tools for processing the information collected by the Intelligence Service through its technical procurement activities is continually updated and developed, and the service has kept the Committee informed of any developments. In 2008, the Committee has emphasised the oversight of the technical procurement activities of the service. The Committee's technical expert has assisted the Committee in inspecting this area.

In collaboration with the Committee, the Secretariat and the Committee's technical expert has, over the course of the year, met with the service to gain a better understanding of the tools used by the service to process information collected through the technical procurement activities, and to further improve the Committee's oversight routines. The service has been most accommodating and has expressed a positive attitude towards the need to facilitate for better external control on the part of the Committee. The service has informed the Committee of the structure, contents, and function of, and administrative procedures associated with, its system. This system has simplified and improved the Committee's oversight of the service's technical information procurement, including the basis on which information is collected, the types of information collected, and how this information is processed by the service.

Under and pursuant to Section 4 of the Intelligence Service Act, the Intelligence Service shall "not on Norwegian territory monitor or in any other concealed manner procure information concerning Norwegian physical or legal persons". This injunction requires that the service's technical procurement activities include routines to intercept and identify Norwegian objects as soon as nationality can be established. The Committee has established an inspection routine geared specifically towards overseeing this aspect.

Inspections carried out in 2008 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.

In 2008, the service also informed the Committee of efforts to establish a multinational collaborative project for several aspects of the technical information procurement. The Committee was informed that the Ministry of Defence has approved the collaboration and that the project will be subject to internal review on the same basis as the technical procurement systems. Procedures have been established for quality assurance and legality assessments, as well as logging systems that facilitate oversight. In addition to making sure the service does not procure information on Norwegian citizens, another key focal area in the Committee's oversight activities will be to ascertain that the activities are subject to national control, in accordance with Section 4 of the intelligence service instructions.

VI. DRAFT AMENDMENTS TO LEGISLATION AND INSTRUCTIONS

In 2008, the Committee has, in a separate report to the Storting, proposed draft amendments to the Act relating to the Monitoring of Intelligence, Surveillance and Security Services of 3 February 1995, no. 7, and the Instructions relating to the Monitoring of Intelligence, Surveillance and Security Services (EOS) laid down by the Storting on 30 May 1995 (EOS Instructions).

The draft amendments were primarily motivated by a need to update certain terms and concepts as a consequence of name changes in and restructuring of the services. In addition, a need to amend the regulations relating to the authority to appoint new employees to the Committee's Secretariat and to determine remuneration has emerged over time. In the

evaluation process, the Committee found it expedient to propose other amendments as well.

Draft amendments to the EOS Act propose that the Committee, within the framework of existing acts and guidelines, carries out its responsibilities independently of the Storting. The Committee is satisfied with its current relationship with the Storting, and in the justification for the draft amendments the Committee specifies that any amendment would only serve to clarify to the public that the Committee, in its day-to-day activities is completely independent of political processes and influences. This is especially valuable in terms of the Committee's oversight activities, because the secrecy to which the EOS services are bound so easily generates suspicion of behind-the-scenes processes and conspiracy theories. The Committee investigates the activities of the services on behalf of the public, and it is absolutely vital that the public has faith in the Committee's objectivity and integrity.

Furthermore, the draft amendments propose that the Storting's Presidium decide on matters involving security clearance for the Committee's members. Currently, the Committee's members are granted security clearance by the National Security Authority (NSM). This practice has instilled faith in the services that the security clearance process is completed in the proper fashion. However, in principle it is unfortunate that one of the services the Committee is supposed to inspect has the authority to decide whether or not a Committee member will be granted security clearance. These considerations may be better preserved by having the NSM carry out the personal evaluation, whereas the Presidium makes a decision on whether to grant security clearance on the basis of that evaluation. The NSM shall retain the authority to grant security clearance to employees in the Committee's Secretariat.

In addition, the draft amendments to the EOS Act propose that the Committee shall contribute to the services upholding and respecting human rights. Following the implementation of the Act relating to the Strengthening of the Status of Human Rights in Norwegian Law of 21 May 1999, no. 30 (the Human Rights Act), international human rights, as well as national principles of justice pertaining to the rights of the individual, have in recent years been operationalised and applied in Norway on a far wider scale than previously. These developments have impacted the Committee's area of oversight as well, and the Committee has felt compelled, in connection with several cases in recent years, to address various problems associated with international human rights with the services. These developments have, in the Committee's view, prompted amendments to the EOS Act, which expressly state that the Committee, in its oversight activities, shall contribute to upholding human rights.

The proposed amendment to the EOS instructions entail updating concepts and references as a consequence of name changes, legislative changes, and organisational changes, including the regulation of inspection duties in the FSA. In addition, the draft amendments propose to transfer the employment and remuneration authority relating to Secretariat staff from the Storting's Presidium to the Committee itself, to amend the Committee's quorum requirements, and to regulate the Committee's access to vesting inspection preparations and the investigation of individual cases in the Secretariat.

VII. ADMINISTRATIVE MATTERS

1. Budget and accounts

The Committee's expenses for 2008 totalled NOK 7,785,000, compared with a budget, including a transfer, of NOK 7,922,000.

2. Staff

Hakon Huus-Hansen was the Head of the Secretariat for the Committee until 31 August 2008. As of 1 September 2008 he has been on leave from his position to act as interim judge. During his absence, Legal Adviser Ingeborg Skonord acts as Head of the Secretariat. Henrik Magnusson worked as a Legal Adviser until 4 May 2008. As of 5 May 2008 he has been on leave from his position to work as adviser to the Parliamentary Ombudsman. Silje Sæterdal Hanssen has been working as a Legal Adviser since 25 August 2008. Senior Executive Officer Lise Enberget is in charge of administrative tasks.

Responsibility for the Committee's remuneration assignment and accounting was transferred from the Storting to the Government Agency for Financial Management (SSØ) as of 1 July 2008. Since the EOS Committee's inception in 1996 the Accounting Section of the Storting has been responsible for the Committee's accounts. However, over the years the Committee has established its own Secretariat, employing four permanent staffmembers. These developments have made the Committee better able to assume greater responsibility for its own accounting and finance management. SSØ offered the chance to implement a more expedient solution for invoicing and wage payment, involving relatively modest costs. The transfer to SSØ meant that the Secretariat staff had to take on more responsibility in terms of invoicing and payments to the Committee's Secretariat, which also entailed improved and continuous control of the Committee's spending.

In 2008, the Committee established a new website – www.eos-utvalget.no – where visitors can find, inter alia, information about the Committee, as well as the annual report for 2007, in English. Furthermore, a brief introduction of the Committee has also been translated to Sami, Spanish, German, French, Russian, Arabic, and Urdu.

Oslo, 17 March 2009

Helga Hernes

Svein Grønnern

Trygve Harvold

Knut Hanselmann

Gunhild Øyangen

Theo Koritzinsky

Ingeborg Skonnord

Appendix 1

INFORMATION PAPER

The Norwegian Parliamentary Intelligence Oversight Committee

About the Committee

The Norwegian Parliamentary Intelligence Oversight Committee (the EOS Committee) is a permanent oversight body for what in daily language is often referred to as "the secret services". The Committee is responsible for continuous oversight of the Norwegian Police Security Service (PST), the Norwegian Intelligence Service (NIS) and the Norwegian National Security Authority (NSM). In Norwegian, "Intelligence, Surveillance and Security" is abbreviated to EOS and these services are therefore often collectively referred to as the "EOS services".

The oversight arrangement is independent of the EOS services and the remainder of the public administration. The members of the Committee are elected by the Storting, and the Committee reports to the Storting in the form of annual reports and special reports. The arrangement was established in 1996.

Continuous oversight is carried out by means of regular inspections of the EOS services, both at their central headquarters and at external units. The Committee also deals with complaints from private individuals and organizations that believe the EOS services have committed injustices against them.

This information paper provides a brief guide to the Committee, its responsibilities and activities.

The Storting has passed a separate Act and Instructions for the Committee.

Appointment and composition of the Committee
The Norwegian Parliamentary Intelligence Oversight Committee has seven members, including the chairman and vice-chairman. The members are elected by the Storting in plenary session on the recommendation of the Storting's Presidium. The term of office is normally five years. The members may be re-elected. Deputies are not elected.

The Committee conducts its day-to-day work independently of the Storting, and members of the Storting are not permitted to be simultaneously members of the Committee. The Storting has emphasized that the Committee should have a broad composition, representing both political experience and experience of other areas of society. The following is a brief presentation of the current members of the Committee:

HELGA HERNES, COMMITTEE CHAIR

Senior Adviser, International Peace Research Institute, Oslo. Former ambassador and state secretary at The Ministry of Foreign Affairs (Labour Party). Elected to the Committee 8 June 2006. Term of office expires 30 June 2009.

SVEIN GRØNNERN, DEPUTY CHAIR

Secretary General, SOS Children's Villages in Norway. Former Secretary General of the Conservative Party. Elected to the Committee 6 June 1996, re-elected 31 May 2001 and 8 June 2006. Term of office expires 30 June 2011.

KJERSTI GRAVER, COMMITTEE MEMBER

Judge at Borgarting Court of Appeals, former Consumer Ombudsman. Elected to the Committee 19 May 1998, re-elected 16 June 1999 and 14 may 2004. Term of office expires 30 June 2009.

TRYGVE HARVOLD, COMMITTEE MEMBER

Managing Director of the Norwegian Legal Database Foundation Lovdata. Elected to the Committee 7 November 2003, re-elected 8 June 2006. Term of office expires 30 June 2011.

GUNHILD ØYANGEN, COMMITTEE MEMBER

Former Minister of Agriculture and member of the Storting (Labour Party). Elected to the Committee 8 June 2006. Term of office expires 30 June 2011.

KNUT HANSELMANN, COMMITTEE MEMBER

Mayor in Askøy, Hordaland. Former member of the Storting (The Progress Party). Elected to the Committee
8 June 2006. Term of office expires 30 June 2011.

THEO KORITZINSKY, COMMITTEE MEMBER

Associate Professor of Social Studies, Oslo University College, former member of the Storting and Chairman of the Socialist Peoples Party. Elected to the Committee
1 July 2007. Term of office expires 30 June 2009.

The area of and the purpose of the oversight

The task of the Committee is to oversee the intelligence, surveillance and security services performed or managed by the public authorities whose purpose is to safeguard national security interests. Intelligence, surveillance and security services for other purposes, ordinary criminal investigation and traffic surveillance, are not included in the area of oversight.

The area of oversight is not associated with specific organizational entities. It is therefore not of decisive importance for the oversight authority which bodies or agencies perform EOS services at any given time. These duties are currently assigned to the Norwegian Police Security Service, the Norwegian National Security Authority and the Norwegian Intelligence Service. Consequently, the Committee's continuous oversight is currently conducted in relation to these services. However, the Committee may also conduct investigations in other parts of the public service if this is found appropriate for clarification of the facts of a case. The purpose of the oversight is primarily that of safeguarding the security of individuals under the law. It is the Committee's job to establish whether anyone is being subjected to unjust treatment and to prevent this from occurring, and also to ensure that the EOS services do not make use of more intrusive methods than are necessary in the circumstances. The Committee is also required to carry out general oversight to ensure that the EOS services keep their activities within the legislative framework.

The responsibility for oversight does not embrace activities involving persons who are not resident in Norway or organizations that have no address in this country. The same applies to activities involving foreign citizens whose residence in Norway is associated with service for a foreign state. This exception is particularly intended for diplomatic personnel. However, the Committee may look into these areas too if special grounds so indicate. Public prosecutors and the Director General of Public Prosecutions are also exempt from the Committee's oversight.

What the Committee can do

The Committee can express its views on matters or circumstances that it investigates in the course of its oversight activities and make recommendations to the EOS services, for example that a matter should be reconsidered or that a measure or practice should be discontinued. However, the Committee has no authority to issue instructions or make decisions concerning the services.

In its reports to the Storting concerning oversight activities, the Committee may draw attention to circumstances or issues in the EOS services that it regards as being of current interest. This provides the Storting with a basis for considering whether, for example, changes should be made in practice or legislation.

The Committee has a broad right to inspect government archives and registers and an equivalent right of access to government premises and installations of all kinds. This is necessary to enable the Committee to perform its oversight responsibility. The Committee may summon employees of the EOS services and other government employees and private persons to give evidence orally to the Committee. The Committee may also require evidence to be taken in court. The Committee is also entitled to use expert assistance in oversight activities when it finds this appropriate. This is done to a certain extent within the field of data and telecommunications, particularly in overseeing the Norwegian Intelligence Service.

The Committee exercises oversight in two ways, by means of inspection and by investigating complaints and matters raised on its own initiative.

Inspections

The Committee inspects the headquarters of the PST six times a year, the NSM four times a year and the NIS twice a year. More inspections may be carried out if necessary. The services' external units are also regularly inspected. Prior notice is given of inspections but inspections may also be carried out without prior notice.

The PST is managed from the Central Unit (DSE). The service has units in all police districts. The main duties of the Service involve prevention and investigation of illegal intelligence activities, terrorism and proliferation of weapons of mass destruction. The Committee's inspection of the PST is concentrated around criteria and practice for registering persons in the Service's registers for preventive purposes. The oversight also includes the Service's investigation activities, including the use of various concealed coercive measures, such as wiretapping and room tapping. The Service – and the oversight activities – are primarily directed towards persons.

The NSM is organised as an independent directorate under the Department of Defence. The Service's responsibilities are of a preventive nature. It is not engaged in investigation. The Committee's most important duty in relation to this service is to oversee processing and decisions in matters concerning security clearance. The Committee's area of oversight includes all clearance authorities within both the defence establishment and the civil service. In its inspections of the Headquarters of the NSM, the Committee is routinely shown the decisions in security clearance cases where appeals have been unsuccessful. The Committee also makes regular spot checks on decisions concerning refusal or withdrawal of clearances that have not been appealed. Another important oversight responsibility involves ensuring that the Services' preventive communications monitoring is kept within the framework laid down in the Security Act and regulations issued pursuant to the Act. This includes prohibition of monitoring of private communications and requirements regarding the destruction of material according to specific time limits.

The statutory duty of the Intelligence Service is to gather, process and analyse information regarding Norwegian security interests in relation to foreign states, organizations or individuals. This means that the activities of the Service are directed towards external threats, i.e. threats outside Norway's borders. The Service has posts for gathering and analysing electronic communications, and has units at the High Commands of the armed

forces. It cooperates with corresponding services in other countries. A major responsibility in overseeing the NIS involves ensuring compliance with the provisions of the Act relating to the Norwegian Intelligence Service prohibiting the surveillance of Norwegian natural or legal persons on Norwegian territory and requiring that the service be under national control. The oversight is characterized by the high level of technology within electronic intelligence. The Committee therefore makes broad use of expert assistance in overseeing this service.

The Committee's consideration of complaints and matters raised by the Committee itself
Anyone who believes that the EOS services may have committed injustices against him or her may complain to the EOS Committee. All complaints that fall under the area of oversight and that show a certain basis in fact are investigated. A complaint should be made in writing and sent to the Committee. If this is difficult, help in formulating a complaint may be provided by prior arrangement. It is important that grounds are given for the complaint and that the complaint is made as explicit as possible.

No explicit time limit applies for complaints to the Committee. However, the Committee is cautious of investigating complaints concerning matters of considerable age unless they can be assumed to have current importance for the complainant and it has been difficult to submit the complaint earlier. Complaints are investigated in the service against which they are directed. This is partly carried out in writing, partly orally in the form of inspections and partly by checking archives and registers. Complaints to the Committee are dealt with in confidence but, when a complaint is investigated, the service concerned is informed. If the investigation reveals grounds for criticism, this is indicated in a written statement to the service concerned. The Committee has no authority to instruct the services to take specific action concerning a matter, but may express its opinion, and may make recommendations to the services, for example, to reconsider a matter.

Even if no complaint has been submitted, the Committee shall on its own initiative investigate matters or circumstances that it finds reason to examine more closely in view of its oversight capacity. It is stressed as being particularly important that the Committee investigates matters or circumstances that have been the subject of public criticism. A not inconsiderable number of the matters investigated by the Committee are raised on the initiative of the Committee itself.

The Committee has a duty of secrecy
Much of the information the Committee receives in its oversight capacity and in investigating complaints is classified, i.e. subject to secrecy on grounds of national security interests. Classified information cannot be disclosed by the Committee. This sets clear limits for the kind of information the Committee may provide to complainants concerning their investigations and the results of them. In the case of complaints concerning surveillance activities by the PST, the Committee may as a general rule only inform as to whether or not the complaint gives grounds for criticism. Nor may the Committee, pursuant to the Act, inform a complainant that he has not been registered or subjected to surveillance since such an arrangement would provide anyone with the possibility of confirming whether or not he or she was the subject of the Service's attention. The Committee may however request the consent of the service concerned or of the Ministry to provide a more detailed explanation in a specific matter if found to be particularly necessary.

The Committee's reports to the Storting shall be unclassified. If the Committee considers that the Storting should be acquainted with classified information in a matter, the Committee shall bring this to the attention of the Storting. It is then for the Storting to decide whether it will procure the information.

Postal address: Stortinget, 0026 Oslo

Office address: Akersgata 8

Telephone: 00 47 23 31 09 30 – Telefax: 00 47 23 31 09 40
E-mail: post@eos-utvalget.no
Website: www.eos-utvalget.no

Appendix 2

Act relating to the Oversight of Intelligence, Surveillance and Security Services

Section 1. *The oversight agency and the oversight area*

The Storting shall elect a committee for the oversight of intelligence, surveillance and security services carried out by, under the control of or on the authority of the public administration.

Such oversight shall not apply to any superior prosecuting authority.

The Public Administration Act and the Freedom of Information Act shall not apply to the activities of the Committee, with the exception of the Public Administration Act's provisions concerning disqualification.

The Storting shall issue an ordinary directive concerning the activities of the Oversight Committee within the framework of this Act and lay down provisions concerning its composition, period of office and secretariat.

The Committee exercises its mandate independently, outside the direct control of the Storting, but within the framework of laws and its directives. The Storting may, however, in regular joint decisions (Storting resolutions) order the committee to undertake specified investigations within the oversight mandate of the Committee, and under the auspices of the rules and framework which otherwise govern the Committee's activities.

Section 2. *Purpose*

The purpose of the oversight is:

1) to ascertain and prevent any exercise of injustice against any person, and to ensure that the means of intervention employed do not exceed those required under the circumstances,
2. to ensure that the activities do not involve undue damage to civic life,
3. to ensure that the activities are kept within the framework of statute law, administrative or military directives and non-statutory law.

The Committee shall show consideration for national security and relations with foreign powers.

The purpose is purely to oversee. The Committee may not instruct the bodies it oversees or be used by these for consultations.

Section 3. *The responsibilities of the Oversight Committee*

The Committee shall regularly oversee the practice of intelligence, surveillance and security services in public and military administration.

The Committee shall investigate all complaints from persons and organisations. The Committee shall on its own initiative deal with all matters and factors that it finds appropriate to its purpose, and particularly matters that have been subject to public criticism. Factors shall here be understood to include regulations, directives and established practice.

When this serves the clarification of matters or factors that the Committee investigates by virtue of its mandate, the Committee's investigations may exceed the framework defined in Section 1, first subsection, cf. Section 2.

Section 4. *Right of inspection, etc.*

In pursuing its duties, the Committee may demand access to the administration's archives and registers, premises, and installations and of all kinds. Establishments, etc. that are more than 50 per cent publicly owned shall be subject to the same right of inspection.

All employees of the administration shall on request procure all materials, equipment, etc. that may have significance for effectuation of the inspection. Other persons shall have the same duty with regard to materials, equipment, etc. that they have received from public bodies.

Section 5. *Statements, obligation to appear, etc.*

All persons summoned to appear before the Committee are obliged to do so.

Persons making complaints and other private persons treated as parties to the case may at each stage of the proceedings be assisted by a lawyer or other representative to the extent that this may be done without classified information thereby becoming known to the representative. Employees and former employees of the administration shall have the same right in matters that may result in criticism of them.

All persons who are or have been in the employ of the administration are obliged to give evidence to the Committee concerning all matters experienced in the course of their duties.

An obligatory statement must not be used against any person or be produced in court without his consent in criminal proceedings against the person giving such statements.

The Committee may apply for a judicial recording of evidence pursuant to Section 43, second subsection, of the Courts of Justice Act. Sections 22-1 and 22-3 of the Civil Procedure Act shall not apply. Court hearings shall be held in camera and the proceedings shall be kept secret. The proceedings shall be kept secret until the Committee or the competent ministry decides otherwise, cf. Sections 8 and 9.

Section 6. *Ministers and ministries*

The provisions laid down in Sections 4 and 5 do not apply to Ministers, ministries, or their civil servants and senior officials, except in connection with the clearance and authorisation of persons and enterprises for handling classified information.

Section 7. (Repealed by the Act of 3 Dec. 1999 no. 82 (in force from 15 Oct. 2000 in acc. with Decree of 22 Sep. 2000 no. 958).)

Section 8. *Statements and notifications*

1. Statements to complainants shall be unclassified. Information concerning whether any person has been subjected to surveillance activities shall be regarded as classified unless otherwise decided. Statements to the administration shall be classified according to their contents.

   The Committee shall decide the extent to which its unclassified statements or unclassified parts of statements shall be made public. If it is assumed that making a statement public will result in revealing the identity of the complainant, the consent of this person shall first be obtained.

2. The Committee submits annual reports to the Storting about its activities. Such reports may also be submitted if factors are revealed that should be made known to the Storting immediately. Such reports and their annexes shall be unclassified.

Section 9. *Duty of secrecy, etc.*

With the exception of matters provided for in Section 8, the Committee and its secretariat are bound to observe a duty of secrecy unless otherwise decided.

The Committee's members and secretariat are bound by regulations concerning the handling of documents, etc. that must be protected for security reasons. They shall be authorised for the highest level of national security classification and according to treaties to which Norway is a signatory. The Presidium of the Storting is the security clearance authority for the Committee members. Background checks will be performed by the National Security Authority.

Should the Committee be in doubt as to the classification of information in statements or reports, or be of the opinion that certain information should be declassified or given a lower classification, the issue shall be put before the competent agency or ministry. The administration's decision is binding on the Committee.

Section 10. *Assistance etc.*

The Committee may engage assistance.

The provisions of the Act shall apply correspondingly to persons engaged to assist the Committee and to legal representatives appointed pursuant to Section 7. However, such persons shall only be authorised for a level of security classification appropriate to the assignment concerned.

Section 11. *Penalties*

Wilful or grossly negligent infringements of Section 4, first and third subsections of Section 5, first and second subsections of Section 9 and the second subsection of Section 10 of this Act shall render a person liable to fines or imprisonment for a term not exceeding one year, unless stricter penal provisions apply.

Section 12. *Entry into force*

This Act shall enter into force immediately.

Appendix 3

Directive relating to oversight of the intelligence, surveillance and security services (EOS)

Section 1. *On the Oversight Committee and its secretariat*

The Committee shall have seven members including the chair and deputy chair, all elected by the Storting, on the recommendation of the Presidium of the Storting, for a period of no more than five years. Steps should be taken to avoid replacing more than four members at the same time.

The members of the Committee shall have the highest and authorisation, both nationally and according to treaties to which Norway is a signatory.

Remuneration to the Committee's members shall be determined by the Presidium of the Storting.

The chair of the Committee's secretariat shall be appointed and the chair's remuneration stipulated by the Presidium of the Storting on the basis of a recommendation from the Committee. Appointment and stipulation of the remuneration of the other secretariat members shall be made by the Committee. More detailed rules on the appointment procedure and the right to delegate the Committee's authority will be stipulated in personnel regulations to be approved by the Presidium of the Storting. The provision in the second subsection applies similarly to all employees in the secretariat.

Section 2. *Quorum and working procedures*

The Committee has a quorum when five members are present. The Committee shall as a rule function jointly, but may divide itself during inspection of service locations or installations.

In connection with particularly extensive investigations, the procurement of statements, inspections of premises, etc. may be carried out by the secretary and one or more members. The same applies in cases where such procurement by the full committee would require excessive work or expense. In connection with hearings, as mentioned in this Section, the Committee may engage assistance. It is then sufficient that the secretary or a single member participates.

The Committee may also otherwise engage assistance when special expertise is required.

Persons who have previously functioned in the intelligence, surveillance and security services may not be engaged to provide assistance.

Section 3. *Procedure regulations*

The secretariat keeps a case journal and minute book. Decisions and dissenting opinions shall appear from the minute book.

Statements and notes which appear or are entered in the minutes during oversight activities are not considered made unless communicated in writing.

Section 4. *Oversight limitations etc.*

The oversight activities do not include activities which concern persons or organisations not domiciled in Norway, or foreigners whose stay in Norway is in the service of a foreign state. The Committee can, however, exercise oversight in cases as mentioned above when special reasons so indicate.

The oversight activities should be exercised so that they pose the least possible disadvantage for the current activities of the services. The ministry appointed by the King can, in times of crisis and war, suspend the oversight activities in whole or in part until the Storting decides otherwise. The Storting shall be notified of such suspension immediately.

Section 5. *Access limitations*

The Committee shall not seek more extensive access to classified information than warranted by its oversight purposes. Insofar as possible, the concern for protection of sources and safeguarding of information received from abroad shall be observed.

Information received shall not be communicated to other authorised personnel or to other public bodies which are not already privy to them unless there is an official need for this, and it is necessary as a result of the oversight purposes or results from case processing provisions in Section 9. If in doubt, the provider of the information should be consulted.

Section 6. *Disputes concerning access to information and oversight*

The decisions of the Committee concerning what it shall seek access to and concerning the scope and extent of the oversight shall be binding on the administration. The responsible personnel at the service location concerned may demand that a reasoned protest against such decisions be recorded in the minutes. Protests following such decisions may be submitted by the head of the respective service and the Chief of Defence.

The protest shall, as mentioned here, be included in or enclosed with the Committee's annual report.

Section 7. *On the oversight and statements in general*

The Committee shall adhere to the principle relating to subsequent oversight. The Committee may, however, demand access to and make statements about current cases.

The Committee shall base its oversight and the formulation of its statements on the principles set down in Section 10, first subsection and Section 10, second subsection, first, third and fourth sentence, and Section 11 of the Act concerning the Storting's Ombudsman for public administration. The Committee may also propose improvements in administrative and organisational arrangements and routines where these can make oversight easier or safeguard against injustice being done.

Before making a statement in cases which may result in criticism or opinions directed at the administration, the head of the service in question shall be given the opportunity to make a statement on the issues raised by the case.

Statements to the administration shall be directed to the head of the service or body in question, or to the Chief of Defence or the competent ministry if the statement relates to matters they should be informed of as the commanding and supervisory authorities.

In connection with statements which contain requests to implement measures or make decisions, the recipient shall be asked to report on any measures taken.

Section 8. *On complaints*

On receipt of complaints, the Committee shall conduct such investigations of the administration as are appropriate in relation to the complaint. The Committee shall decide whether the complaint gives sufficient grounds for further action before making a statement.

Statements to complainants should be as complete as possible without revealing classified information. Statements in response to complaints against the Police Security Service concerning surveillance activities shall however only state whether or not the complaint

contained valid grounds for criticism. If the Committee holds the view that a complainant should be given a more detailed explanation, it shall propose this to the Ministry concerned.

If a complaint contains valid grounds for criticism or other comments, a reasoned statement shall be addressed to the head of the service concerned or to the ministry concerned. Statements concerning complaints shall also otherwise always be sent to the head of the service against which the complaint is made.

Section 9. *Procedures*

Conversations with private individuals shall be in the form of an examination unless they are meant to merely brief the individual. Conversations with administration personnel shall be in the form of an examination when the Committee sees reason for doing so or the civil servant so requests. In cases which may result in criticism being levied at individual civil servants, the examination form should generally be used.

The person who is being examined shall be informed of his or her rights and obligations, cf. Section 5 of the Act relating to the Oversight of Intelligence, Surveillance and Security Services. In connection with examinations that may result in criticism of the administration's personnel and former employees, said individuals may also receive the assistance of an elected union representative who has been authorised according to the Security Act with pertinent regulations. The statement shall be read aloud before being approved and signed.

Individuals who may become subject to criticism from the Committee should be notified if they are not already familiar with the case. They are entitled to familiarise themselves with the Committee's unclassified material and with any classified material they are authorised to access, insofar as this does not impede the investigations.

Anyone who submits a statement shall be presented with evidence and claims which do not correlate with their own evidence and claims, insofar as these are unclassified or the person has authorised access.

Section 10. *Investigations at the ministries*

The Committee cannot demand access to the ministries' internal documents.

Should the Committee desire information or statements from a ministry or its personnel in other cases than those which concern the ministry's handling of clearance and authorisation of persons and enterprises, these shall be obtained in writing from the ministry.

Section 11. *Inspection*

1. Responsibilities for inspection are as follows:
   a) For *the intelligence service:* to ensure that activities are carried out within the framework of the service's established responsibilities, and that no injustice is done to any person.
   b) For *the National Security Authority:* to ensure that activities are carried out within the framework of the service's established responsibilities, to oversee clearance matters in relation to persons and enterprises for which clearance has been denied, revoked, reduced or suspended by the clearance authorities, and also to ensure that no injustice is done to any person.
   c) For *the Police Security Service :* to oversee that the service's handling of preventive cases and investigations, its use of concealed coercive measures, its processing of personal data, and the exchange of information with domestic and foreign collaborative partners is carried out in accordance with current regulations, and meets the requirements for satisfactory routines within the framework of the purpose stated

in Section 2 of the Act.

d) For *the Defence Security Section:* to oversee that the service's exercise of personnel security clearance activities and other security clearance activities are kept within the framework of laws and regulations and the service's established responsibilities, and also to ensure that no injustice is done to any person.

e) For all services*:* to ensure that the cooperation and exchange of information between the services is kept within the framework of service needs and applicable regulations.

2. Inspection activities shall, as a minimum, involve:

a) half-yearly inspections of the Intelligence Service, involving accounts of current activities and such inspection as is found necessary.

b) quarterly inspections of the National Security Authority, involving a review of matters mentioned under 1 b and such inspection as is found necessary.

c) Six inspections per year of the Central Unit of the Police Security Service, involving a review of new cases and the current use of concealed coercive measures, including at least ten random checks in archives and registers at each inspection, and involving a review of all current cases at least twice a year.

d) Three inspections per year of the Defence Security Service, including a review of the agency as a clearance authority, and a review of other security-related activities as found necessary.

e) annual inspection of at least four police districts, at least two Intelligence Service Units and/or intelligence/security services at military units and of the personnel security service of at least two ministries/government agencies.

f) inspection of measures implemented on its own initiative by the remainder of the police force and by other bodies or institutions that assist the Police Security Service.

g) other inspection activities indicated by the purpose of the Act.

Section 12. *Information to the public*

Within the framework of the third paragraph of Section 9 of the Act cf. Section 8, paragraph 1, the Committee shall decide what information shall be made public concerning matters on which the Committee has commented. When mentioning specific persons, consideration shall be given to protection of privacy, including persons not issuing complaints. Civil servants shall not be named or in any other way identified except by authority of the ministry concerned.

In addition, the chair or whoever the Committee authorises can inform the public of whether a case is being investigated and if the processing has been completed or when it will be completed.

Section 13. *Relationship to the Storting*

1. The provision in Section 12, first subsection, correspondingly applies to the Committee's notifications and annual reports to the Storting.
2. Should the Committee find that the consideration for the Storting's supervision of the administration dictates that the Storting should familiarise itself with classified information in a case or a matter the Committee has investigated, the Committee must notify the Storting specifically or in the annual report. The same applies to any need for further investigation into matters which the Committee itself cannot pursue further.
3. By 1 April every year, the Committee shall report its activities in the preceding year to the

Storting.

The annual report should include:

a) an overview of the composition of the Committee, its meeting activities and expenses.

b) a statement concerning implemented supervision activities and the result of said activities.

c) an overview of complaints by type and service branch, indicating what the complaints resulted in.

d) a statement concerning cases and matters raised on the Committee's own initiative.

e) a statement concerning any measures the Committee has requested be implemented and what these measures led to, cf. Section 6, fifth subsection.

f) a statement concerning any protests pursuant to Section 5.

g) a statement concerning any cases or matters which should be put before the Storting.

h) the Committee's general experiences from the oversight activities and the regulations and any need for changes.

Section 14. *Financial management, expense reimbursement for persons summoned before the Committee and experts*

1. The Committee is responsible for the financial management of the Committee's activities, and stipulates its own financial management directive. The directive shall be approved by the Presidium of the Storting.
2. Anyone summoned before the Committee is entitled to reimbursement of any travel expenses d in accordance with the State travel allowance scale. Loss of income is reimbursed in accordance with the rules for witnesses in court.
3. Experts are remunerated in accordance with the courts' fee regulations. Higher fees can be agreed. Other persons assisting the Committee are reimbursed in accordance with the Committee scale unless otherwise agreed.

Appendix 4

Stortinget
EOS-utvalget | Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste

0026 Oslo

January 13, 2009

Our ref.: 2008000050 Your ref.:

Draft amendments to EOS Committee regulations

The EOS Committee hereby submits to the Storting its proposal for draft amendments to the Act relating to the Monitoring of Intelligence, Surveillance and Security Services no. 7 of 1995 (the EOS Act) and the Instructions for Monitoring of Intelligence, Surveillance and Security Services (EOS) established by the Storting on 30 May 1995 (the EOS instructions).

1. On administrative procedures for addressing proposals

The Committee has not previously addressed any issues relating to amendments to the EOS Act and the EOS instructions, and it is thus somewhat uncertain as to the administrative procedures deemed appropriate by the Storting in matters pertaining to amendments to legislation and regulations applying to one of the Storting's external organs, including whether a working committee ought to be established to review the draft amendments or parts thereof. The Committee has opted to initialise the process by way of this letter, wherein a detailed account is provided for each of the individual amendments proposed by the Committee. The Committee would furthermore like to emphasise that it will follow any and all advice and recommendations as to the proper procedure in this matter.

Prior to drafting this letter, the Committee submitted the draft amendments affecting the various services to the Intelligence Service, the Police Security Service, the National Security Authority, and the Defence Security Service (formerly the Armed Forces' Security Section), as well as the Ministries of Justice and Defence. The services and ministries responded with some comments to the draft amendments, which are appended hereto. As stated in the letter from the Ministry of Justice, dated 2 January 2009, the ministry prefers to refrain from commenting, and instead await being contacted by the Storting in connection with amendments to the regulations. Comments from the services and the Ministry of Defence have been included in the description of the draft amendments in question.

2. General information about the draft amendments

An update of the EOS instructions has been necessary for a long time. This need for amendment is in part caused by name changes in and restructuring of the services taking place after the implementation of the EOS instructions, and the new legislation implemented for the services, in particular the implementation of the Security Act, caused some references and terms in the instructions to become incorrect. The other main motivation for submitting

these draft amendments to the Storting is the need that has emerged over time to amend the regulations relating to the authority to appoint new employees to the Committee's Secretariat and to determine remuneration. The draft amendments propose that this authority be transferred from the Presidium of the Storting to the Committee. This amendment will affect the staff of the Committee Secretariat (with the exception of the Head of the Secretariat).

In the evaluation process, the Committee also reviewed several other issues in terms of potential amendments, with the aim of being able to submit a collective proposal to the Storting regarding draft amendments to the all regulations pertaining to the Committee. After completing its evaluation, the Committee found grounds to propose two amendments to the EOS Act. One of the proposed amendments codifies that the Committee, within the framework of applicable legislation and regulations, shall execute its responsibilities independently of the Storting. The other proposed amendment codifies that the security clearance of Committee members shall be subject to a decision by the Presidium of the Storting (following vetting of personnel carried out by the National Security Authority).

The Committee also reviewed the issue of whether one should amend the Section regarding the purpose of the EOS Act to include provisions stipulating that the Committee, in its oversight activities, should contribute to the services upholding and respecting human rights in their activities. The Committee concluded that several arguments exist in favour of including such a provision and has taken the liberty of proposing a possible text.

In addition, the Committee further proposes to amend the EOS instructions, and the draft amendments include amendments to the quorum requirements of the Committee, as well as amendments to regulate the Committee's access to hand over inspection preparations and investigation of individual cases to the Secretariat.

3. Outline of the draft amendments

Proposals for amendments to the EOS Act:
- Amendment to Section 1, Subsection 4 specifying that the Committee, within the framework of existing legislation and instructions, shall execute its responsibilities independently of the Storting.

- Amendment to Section 9, adding a provision stating that the Storting's Presidium shall make decisions to grant security clearance to the Committee's members.

- Amendment to Section 2, no. 1, which specifies that the Committee shall contribute to the services respecting human rights.

Proposals for amendments to the EOS instructions:
- Updates of concepts and references necessitated by name changes, legislative changes, and organisational changes, including the codification of inspection duties in the Armed Forces' Security Section , as well as some clarifications (Sections 6, 8, 9, 11, and 12).

- Transferring the employment and remuneration authority relating to Secretariat staff from the Storting's Presidium to the Committee (Sections 1 and 14).

- Amendments to the Committee's quorum requirements and codification of the Committee's access to hand over inspection preparations and investigation of individual cases to the Secretariat (Sections 1 and 2).

4. Proposals pertaining to amendments to the EOS Act

4.1. Provision concerning the relation between the Committee and the Storting

At present, the EOS Act does not include any provisions pertaining to the relation between the Committee and the Storting in the day-to-day oversight activities – outside of Section 1, Subsection 4, which stipulates that the Storting shall issue instructions concerning the activities of the Committee.

The EOS Act (and the EOS instructions) is based on the recommendations of the Skauge Committee, established by the Official Norwegian Report NOU 1994:4, Inspecting the Secret Services. The recommendations of the Skauge Committee and the draft legislation was, in the main, supported and carried through to the legislative proposition, Proposition no. 83 to the Odelsting (1993-94). The review by the Storting did not entail significant changes, nor was there much debate as to the role of the Committee in relation to the Storting, cf. the recommendations to the Odelsting no. 11 (1994-95) and Legal Gazette (1994-95) p. 141. One can thus conclude that the recommendations of the Skauge Committee on this issue constitute the preparatory documents of the EOS Act.

The recommendations of the Skauge Committee included a thorough discussion of various constitutional issues associated with the establishment of a parliamentary anchored oversight organ for the EOS services. The Skauge Committee emphasised that an oversight organ of this nature would have to be independent of both the EOS services and the administrative authorities. This was achieved by implementing provisions stipulating that the Committee shall not have the authority to instruct the services, but merely to express its opinion, that the Committee shall report to the Storting, that its oversight of the services shall be retrospective, and that the services may not use the Committee as an external consultant.

The recommendations further discussed the relation between the Committee and the Storting, cf. Chapter 4.5, especially items 4.5.4 and 4.6 concerning the Committee's relation with the Standing Committee on Scrutiny and Constitutional Affairs. A clear distinction was made between parliamentary oversight, which is the sole responsibility of the Storting, and parliamentary anchored external oversight. Item 4.5.4 of the recommendations states that in terms of parliamentary oversight, the only function of a parliamentary appointed external oversight organ should be to facilitate for greater efficiency in the parliamentary oversight, and that no restrictions or limitations should be placed on said parliamentary oversight. In addition to this, the primary responsibility of the Committee would be to engage in oversight activities of a purely legislative nature, particularly in terms of the rights of individuals. Outside of these stipulations, the relation between the Committee and the Storting is not further discussed. It is possible that the Skauge Committee believed that its proposed legislation and instructions established a framework so detailed for the oversight activities that there would be no leeway for the Storting to issue instructions on individual cases without resorting to amend the existing regulations. However, the shortcomings could also be a result of the legislation being temporary and subject to evaluation at a later date. Furthermore, it represented a new form of oversight activity in a highly sensitive administrative area.

The main motivation behind codifying the principle of the Committee's execution of its oversight activities independently of the Storting, is that this represents an outward manifestation of the Committee's detachment from political process and influences in its daily activities. This is especially valuable in the Committee's area of oversight, because the secrecy to which the EOS services are bound so easily generates suspicion of behind-the-scenes processes and conspiracy theories. The Committee investigates the activities of the services on behalf of the public, and the public's trust in the Committee's objectivity and integrity is absolutely vital.

As the Parliamentary Ombudsman, the EOS Committee is a part of the Storting's external supervision machinery. Section 2 of the Act relating to the Parliamentary Ombudsman stipulates that the Storting shall issue a general directive for the functions of the Ombudsman, but apart from this, the Ombudsman shall execute his duties "autonomously and independently of the Storting". Provisions equal to the provisions of Section 2 of the Act relating to the Parliamentary Ombudsman would, in the Committee's opinion, contribute to strengthening the individual's trust in the Committee.

Nor can it be disregarded that provisions of this nature could be beneficial for the Storting, for example during volatile political climates. However, the Committee emphasises that the motivation for proposing amendments similar to the provisions established for the Ombudsman is not the result of the Committee experiencing its relation to the Storting as problematic. Nor has the Committee ever experienced that its standing is different from that of the Ombudsman in this regard, be it formally speaking, or in practice. Through reviews of its reports by the Standing Committee on Scrutiny and Constitutional Affairs, and by a plenary session of the Storting, the Committee receives signals indicating how the Storting believes the Committee's oversight ought to be organised and prioritised. These signals are useful, and valuable, and the Storing only give guidance in a cautious and principled form. It is the view of the Committee that if the Storting were to request the Committee's investigations into a specific matter, this too, would be unproblematic, provided that the case falls within the scope of the Committee's mandate and does not displace the resources necessary to carry out the Committee's responsibilities pursuant to applicable legislation. The Committee would also like to emphasise that its close dialogue with the Storting is important, because the Committee derives its democratic legitimacy from the Storting. However, if the Storting were to instruct the Committee to refrain from investigating a matter or to cease ongoing investigations, this would conflict with the Committees independence and integrity. This would also conflict with the Committee's mandate and right to initiate investigations ascribed to the Committee by law. Similar issues were debated by the Schei Committee, which reviewed the institution of the Parliamentary Ombudsman in the late seventies. Quoting from the Schei Committee recommendations (Doc. 9 (1977-78)) pp. 18 and 19:

> "In excess of what follows from general provisions, the Storting may not issue instructions as to how the individual case is handled or concluded. The Storting may thus not order the Ombudsman to process a case or to refrain from doing so, nor may the Storting intervene in its processing in any other way. As this provision was discussed in the Storting, the discussion touched on the risk that the Storting might interfere with individual cases. The chair on the matter, the President of the Odelsting, Jakob Pettersen, emphasised the danger of the Storting (Odelsting) becoming an appellate authority for cases handled by the Ombudsman. If this became the case in any extent, it would not only make the tasks of the Ombudsman more difficult, but "it would make it virtually impossible for him to carry out similar activities." (Review by the Storting, no. 72 for 1962-63 p. 574, second column).
> With the clear provision in Section 2 of the Act relating to the Parliamentary Ombudsman, there is no general risk that the Storting would attempt to influence the Ombudsman in the handling of individual cases. The risk, if any, lies in the issue pointed out by then Odelting President Jacob Pettersen – that the Storting or the committee reviewing the annual report attempts to review the Ombudsman's position on specific cases. This is a risk that cannot immediately be dismissed. However, this issue cannot be resolved through legislative measures, but must find resolution through the practices of the Storting and the parliamentary agency in question.---"

The Committee believes that the same considerations expressed by the Schei Committee are relevant for the Committee's oversight activities – with the aforementioned reservation

that a request from the Storting to look into a specific case does not necessarily constitute a restriction on the Committee's autonomy. Also, the concern identified in the latter part of the quote above, that some issues relating to the relationship between an external oversight authority and the Storting cannot be solved through legislative measures, but must find resolution through practical arrangements, is still relevant today.

The Parliamentary Ombudsman and the EOS Committee differ in many respects. The Committee is a collegial body, and its primary responsibility is inspection activities, whereas investigating complaints is a minor part of its activities. Its purpose is not solely to investigate whether the rights of individuals have been violated, but also to make sure that the activities of the services are kept within the legal framework to which the services are subject. Most of the information it receives is classified and may not be disclosed to others, and, finally, the Committee operates in an area that may be highly sensitive in terms of security and foreign policy. However, none of these differences represent arguments against codifying the principle that the Committee, within the framework of laws and regulations, shall execute its responsibilities autonomously and independently of the Storting.

In light of the above, the Committee proposes that Section 1, Subsection 4 of the EOS Act r is amended as follows (amendments in italics):

"The Storting shall issue ordinary instructions concerning the activities of the monitory committee within the framework of this Act and lay down provisions concerning its composition, period of office and secretariat. *Within the framework of laws and regulations, the Committee shall execute its duties autonomously and independently of the Storting.*"

4.2. Provision concerning security clearance for the Committee's members

Section 9, Subsection 2, second sentence of the EOS Act (as well as Section 1, Subsection 2 of the EOS instructions) stipulates that the Committee's members shall be authorised for the highest level of national security classification, and that they shall be given authorisation after the election. Similar requirements for the Secretariat staff follow from Section 1, Subsection 3 of the EOS instructions.

Neither the existing provisions, nor the preparatory documents of the EOS Act, give any indication as to who grants security clearance and authorises Committee members. This is assumed to be due to the EOS instructions being adopted prior to the Security Act in 1998.

The current practice is that Committee members, as well as Secretariat staff, are given security clearance by the National Security Authority (NSM). The background for this practice is that Section 23, Subsection 4 of the Security Act of 20 March 1998 no. 10 stipulates that clearance for the highest level of security clearance may only be granted by the NSM. The Committee members have been authorised by the President of the Storting, and the Committee Chair has authorised Secretariat staff.

This practice has probably entailed the services' reliance on the security clearance process is carried out in the proper fashion. However, in principle it is unfortunate that one of the services the Committee is obligated to supervise has the authority to decide whether or not a Committee member is granted security clearance. One possible way of combining these concerns is to vest the responsibility for carrying out the vetting of personnel in the NSM, while having the Presidium make the decision on whether to grant security clearance on basis of that evaluation.

An amendment as described above will require the inclusion of a special provision in the Act relating to security clearance for the Committee's members. The reason for this is that Section 23 of the Security Act stipulates that only the NSM may grant clearance for the

highest level of security clearance. By virtue of being a specific rule, any amendment to the Act as described above would supersede Section 23 of the Security Act, meaning that amendments to the Security Act would not be necessary.

Upon contacting the NSM, the Committee has learned that NATO's directives do not contain any provisions stipulating that clearance for NATO levels of security clearance can only be granted by specially appointed national authorities, cf. the appended copy of the NSM's letter, dated 9 October 2008. In light of this, the Committee believes that the existing fundamental considerations are so compelling that the clearance authority should be transferred to the Storting, but in such a manner that the vetting of personnel will still be carried out by the NSM, as is the case today. Section 3-3 of the Regulations relating to personnel security (FOR 2001-06-29, no. 0722) expressly stipulates that the vetting of personnel for security clearance purposes is carried out by the NSM in all cases. It may still be of value to include this rule in the EOS Act pertaining to security clearance of Committee members.

The draft amendments propose replacing the word "authorised" with "granted clearance", as this is a more accurate term in this context.

Section 1 of the EOS instructions may seem to presuppose that security clearance is granted prior to the election. Today, clearance is granted after the election, but it is possible for the Storting to make informal arrangements with the individual in question ahead of time, so that one can ascertain, with a fair level of certainty, that security clearance will be granted. A more neutral wording could perhaps be expedient in this case. Under no circumstances is a person granted access to classified material before security clearance and authorisation is given. Confer proposal under Item 5.2 for amendments to the EOS instructions.

The Committee proposes that Section 9 of the EOS Act is amended to read as follows (amendments in italics, deletions in parentheses):

"Section 9. *Duty of secrecy, etc.*

With the exception of matters provided for in section 8, the Committee and its secretariat are bound to observe a duty of secrecy unless otherwise decided.

The Committee's members and secretariat are bound by regulations concerning the handling of documents, etc., that must be protected for security reasons. They shall be *granted clearance* (authorised) for the highest level of security classification, both nationally and according to treaties to which Norway is a signatory. *The Presidium of the Storting shall be the clearance authority for Committee members. The vetting of personnel shall be carried out by the National Security Authority.*

If the Committee is in doubt concerning the classification of information given in statements or reports, or holds the view that the classification should be revoked or reduced, it shall submit the question to the agency or ministry concerned. The decision of the administration shall be binding for the Committee."

The fundamental considerations against a service being the clearance authority do not apply to Secretariat staff. No amendment is thus proposed in this regard. The authorising authority should still be the Presidium for the Committee members, and the Committee Chair for Secretariat staff. It is not deemed necessary to codify the party acting as the authorising authority for Committee members and Secretariat staff, respectively.

4.3. Provision on the relation to human rights

Following the implementation of the Act relating to the Strengthening of the Status of Human Rights in Norwegian Law of 21 May 1999, no. 30 (the Human Rights Act), international

human rights, as well as national principles of justice pertaining to the rights of the individual, have in recent years been operationalised and applied in Norway on a far wider scale than previously. These developments have impacted the Committee's area of oversight as well, and the Committee has felt compelled, in connection with several cases in recent years, to address various problems associated with international human rights, especially the European Convention on Human Rights and the practices of the European Court of Human Rights (EMD) with the services.

These developments have raised the issue of whether one should include a provision in the EOS Act, which expressly states that the Committee, in its oversight activities, shall contribute to upholding human rights. This is not strictly necessary, as Section 2 of the Act relating to purpose – both no. 1 regarding the prevention of injustice against any person and ensuring that the services do not employ more invasive measures than is strictly possible, and no. 3 regarding the general provision that the services must act within the framework of law – currently (through the Human Rights Act) cover the inspection of making sure the services uphold and respect human rights.

At the same time, within the area of public administration the Committee has been established to inspect, a clarification of the regulations would, in turn, also clarify the responsibility for making sure that the services respect human rights. In this area, a clarification is deemed to be especially useful, given that the services' responsibilities routinely mean that they find themselves in situations where the rights of the individual conflict with the interests of national security. In balancing these two conflicting considerations, the standing of human rights is critical, and by contributing to increased emphasis on these developments, especially as a consequence of EMD practices, a specification in the provisions regarding purpose, as described above, will be valuable.

The Committee has observed that the significance of human rights was included in the Act relating to the Parliamentary Ombudsman in 2004, by amending the provisions regarding purpose in Section 3 of the Act. In 2007, a second amendment entailed changing the wording of the provision slightly, in addition to including a specific, codified duty to report to the Storting on the status of human rights in the administration. Reference is made to the Recommendations to the Odelsting no. 75 (2006-2007), from which it follows that the background for the 2007 amendments was a request from the Storting in connection with the follow-up of Resolution 1516 (2006) from the Council of Europe Parliamentary Assembly, which gives the parliamentary assemblies in the member states a special responsibility to ensure that national authorities implement decisions from the European Court on Human Rights (EMD).

It is the Committee's experience that issues related to the application of the European Convention on Human Rights outside of the realm of the nation (article 1) and issues related to the right to personal privacy (article 8) are central when inspecting the activities of the services. In addition, articles 10 and 11, regarding freedom of expression and freedom of assembly, respectively, may also become relevant in some cases. The Committee recognises that a need might exist for a more thorough evaluation, if one wants to specify the individual human rights and assess their significance in the Committee's area of oversight, and the Committee will of course be responsive to any further steps in this process requested by the Storting.

However, a possible text to amend the existing legislation is proposed below. Section 110c of the Constitution establishes that it is up to national authorities to "respect and uphold" human rights. In the Committee's area of oversight it is more appropriate to only use the verb "respect", but this should not be taken to hold any particular significance for the content of the text.

Proposed text for Section 2, no. 1 of the EOS Act (amendments in italics):

"The purpose of the monitoring is:

1. to ascertain and prevent any exercise of injustice against any person, and to ensure that the means of intervention employed do not exceed those required under the circumstances*, and endeavour to ensure that the services respect human rights,*

---"

In a letter of 4 November 2008, the Ministry of Defence suggested a different wording to Section 2, no. 1. A copy of this letter is appended hereto. The Committee's proposal that the purpose of the oversight activity is to "endeavour to ensure" that the services respect human rights is based on the wording of the provisions in Section 3 of the Act relating to the Parliamentary Ombudsman. However, the Committee has no reservations about using the wording suggested by the Ministry of Defence, should the Storting deem that it, for the purposes of Committee oversight, is more appropriate to use the term "ensure".

5. Proposals pertaining to amendments to the EOS instructions

5.1. Proposed amendments resulting from legislative amendments and organisational changes within the services (Sections 6, 8, 9, 11, and 12)

Section 6 of the EOS instructions

Section 6 of the EOS instructions regulates the rights of the services to require that any objections to the Committee's decisions concerning what information the Committee wants to access, be recorded in the minutes immediately, as well as who is authorised to submit such objections. This latter provision, specified in Subsection 1, sentence 3, states that only the "Chief of Defence and the Chief of the Norwegian Security Service Police" may submit a following objection. This provision has now been made adequate, as the Armed Forces' Security Section (formerly Headquarters Defence Command Norway/Security Headquarters) ceased to exist as an organisational unit. On 1 January 2003 this authority was replaced by a civilian directorate, the National Security Authority (NSM), and the Armed Forces' Security Section (FSA), currently renamed the Defence Security Service (FOST). Furthermore, today it may seem unnecessary that only the Chief of Defence may submit following objections on behalf of the units of the Armed Forces.

In light of the above, the Committee proposes the following wording for Section 6 of the EOS instructions (amendments in italics, deletions in parentheses):

"**Section 6** *Disputes concerning access to information and monitoring*

The decisions of the Committee concerning what information it shall apply for access to and concerning the scope and extent of the monitoring shall be binding on the administration. The responsible personnel at the duty station concerned may require that a reasoned protest against such decisions be recorded in the minutes. Protests following such decisions may be submitted by *the head of the respective service and the Chief of Defence* (the Chief of Defence and the Chief of the Norwegian Security Service Police)."

In connection with this provision the Committee notes that the special arrangement established for the Intelligence Service in 1999 (cf. Recommendations to the Storting no. 232 (1998-1999) and the subsequent debate on the matter in the session of the Storting on 15 June 1999), in the Committee's view does not need to be formalised at this time. This special arrangement entails that in the event of a dispute with the Intelligence Service regarding access, the Committee's right of access is suspended while the case is presented to the Ministry of Defence, and ultimately to the Storting, if the matter cannot be resolved. The

arrangement has hitherto not been used, and the current procedures for access in the Intelligence Service are followed to satisfaction.

Sections 8, 9, and 11 of the EOS instructions

The EOS Act is systematic consistent, using functional descriptions of the types of services the Committee shall inspect (EOS). This was well-considered, and the objective was to avoid having Committee oversight tied up to specific organisational units. Changing this fundamental approach and the pertaining functional labels is not deemed relevant by the Committee at this time.

In the instructions it has been more difficult to maintain a consistent functional range of terms. In Section 11 especially, which describes the Committee's inspections in detail, names (the institutional labels) have also been used. The benefit of using functional labels is that name changes do not require regulatory amendments. However, as this approach was not fully feasible at the time the instructions were adopted, it is the Committee's opinion that it should be put greater emphasis on making the regulatory framework accessible for lay people. This is also the motivation behind amendments to Section 8. Reference is made to the proposed texts below.

In this regard, the Committee has also considered the proposal from the Police Security Service, dated 22 October 2008, cf. appended copy, that the use of the term surveillance service in the Committee's full name ought to be revised. Given that the Committee's oversight is functionally defined, and consequently not limited to specific organisational units, the Committee thinks it is not expedient to change the reference to the name of the unit or the specification of the area of oversight described in Section 1 of the Act. Furthermore, a consistent implementation of such a change would also require amendments to the wording of the EOS Act.

Section 9, Subsection 2, sentence 2, requires that individuals present to assist a party in the investigation be authorised in accordance with the security instructions. Following the implementation of the Security Act and the abolition of the security instructions, this provision is now incorrect, and a new provision is proposed, containing references to the Security Act, with pertaining instructions.

For Section 11, the Committee proposes that the Defence Security Service (FOST) be identified as an object of inspection on an equal basis with the Intelligence Service, the National Security Authority, and the Police Security Service. The justification for this is as follows: As mentioned above, FOST's functions were part of the previous unit FO/S, which is listed as an object of inspection in the current regulations, Section 11, no. 2 b. The 2003 restructuring indicates that both of the separated parties (NSM and FOST) should be specified as objects of inspection. One should take into account that FOST, since its inception in 2003, has grown substantially and is now, without comparison, the larges clearance authority in Norway. FOST is also responsible for the operative security functions within the Armed Forces, intersecting civilian society. These functions are subject to continual development, and it is vital that the Committee inspects its activities. The Committee's oversight responsibilities are clear today, but prudence and the principle of having the regulations mirror the actual situation to the greatest extent possible indicate that these matters should be codified in the regulations. The Committee proposes that the area of oversight covers the security service as a function (new Section 11 no. 1 d), and that the inspection responsibilities include at least three inspections per year of the headquarters (new Section 11 no. 2, letter d). This entails a codification of the Committee's current practice and rate of inspection.

The Defence Security Service (then the Armed Forces' Security Section) informed the Committee, in a letter of 4 November 2008, that the section would change its name to the Defence Security Service as of 1 January 2009, cf. the appended copy. This was also remarked by the Ministry of Defence, which in a letter of 4 November 2008 proposes that the new name be worked into the Committee's draft amendments. Furthermore, the Ministry of Defence expressed that it is in doubt as to whether FOST should be mentioned specifically in Section 11. The ministry justifies its view by stating that these amendments may give rise to the misunderstanding that FOST is "the fourth EOS service" in line with the Intelligence Service, PST, and the NSM.

The new name of FOST has been included in the draft amendments below. In terms of the ministry's hesitation to mentioning FOST specifically, reference is made to the justification above. Both the fact that FOST's functions previously were a part of FO/S – which is mentioned in the current regulations – and the fact that the enterprise is now referred to as a *service*, are indications that the unit is subject to inspection based on the instructions.

The remaining draft amendments, to Section 11 no. 1, letters b), c), and d) are proposed in order to have the regulations correspond better to the terms used in the Security Act and current case types and methods used by the Police Security Service, and to make sure that the instructions reflect the fact that the services currently have formal regulations in place, to which their activities are subject.

The Committee evaluated whether the minimum number of inspections for the National Security Authority should be reduced to three, given that so many clearance cases are handled by FOST. However, the NorCERT department of the NSM grows ever more important, and the material is technically challenging. This department supervises key parts of the digital infrastructure in various technical approaches and methods. NorCERT requires at least one inspection per year, which in actual fact reduces the remaining inspection activities at the NSM. The Committee has thus concluded that the rate of inspection should be maintained.

In order to live up to its inspection responsibilities, the Committee currently carry out three inspections every year of the Intelligence Service, whereas the annual minimum number of inspections, pursuant to Section 11, no. 2, letter a) of the instructions, is two inspections. The Committee did not deem it necessary to propose an increase in the minimum number of inspections in this regard, as the current minimum has the advantage of allowing for greater flexibility.

In light of the above, the Committee thus proposes that Sections 8, 9, and 11 be amended to read as follows (amendments in italics, deletions in parentheses):

"**Section 8.** *On complaints*

On receipt of complaints, the Committee shall make such investigations of the administration as are appropriate in relation to the complaint. The Committee shall decide whether the complaint gives sufficient grounds for further action before making a statement.

Statements to complainants should be as complete as possible without revealing classified information. Statements in response to complaints against the *Police Security Service* (surveillance service) concerning surveillance activities shall however only declare whether or not the complaint contained valid grounds for criticism. If the Committee holds the view that a complainant should be given a more detailed explanation, it shall propose this to the Ministry concerned.

If a complaint contains valid grounds for criticism or other comments, a reasoned statement shall be addressed to the head of the service concerned or to the Ministry concerned. Statements concerning

complaints shall also otherwise always be sent to the head of the service against which the complaint is made.”

“**Section 9.** *Procedures (Subsection 2)*

The person who is being examined shall be informed of his or her rights and obligations, cf. Section 5 of the Act relating to the Monitoring of Intelligence, Surveillance and Security Services. In connection with examinations that may result in criticism of them, the administration’s personnel and former employees may also receive the assistance of an elected union representative who has been authorised according to the *Security Act with pertaining instructions* (security instructions). The statement shall be read aloud before being approved and signed.

---”

“**Section 11.** *Inspection*

1. Responsibilities for inspection are as follows:
   a) For the intelligence service: to ensure that activities are held within the framework of the service’s established responsibilities, and that no injustice is done to any person.
   b) For the *National Security Authority* (security service): to ensure that activities are held within the framework of the service’s established responsibilities, to monitor clearance matters in relation to persons and enterprises for which clearance *has been denied, revoked, reduced or suspended by the clearance authorities* (is advised against by the security staff or refused or revoked by the clearance authority), and also to ensure that no injustice is done to any person.
   c) For the *Police Security Service* (surveillance service): to monitor *that the service’s handling of preventive cases and investigations, its use of concealed coercive measures, its processing of personal data, and the exchange of information with domestic and foreign collaborative partners* (surveillance matters, operations and measures for combating terrorist activities by means of electronic surveillance and mail surveillance and to monitor to ensure that the collection, processing, registering and filing of information concerning Norwegian residents and organisations) is carried out in accordance with current regulations, and meets the requirements for satisfactory routines within the framework of the purpose stated in section 2 of the Act.
   d) For the Defence Security Section: to monitor that the service’s execution of personnel security clearance activities and other security clearance activities are kept within the framework of laws and regulations and the service’s established responsibilities, and also to ensure that no injustice is done to any person.
   (d) *e*) For all services: to ensure that the cooperation and exchange of information between the services is held within the framework of service needs *and applicable regulations.*
2. Inspection activities shall at least involve:
   a) half-yearly inspections of the *Intelligence Service* (central intelligence staff), involving accounts of current activities and such inspection as is found necessary.
   b) quarterly inspections of the *National Security Authority* (security staff), involving a review of matters mentioned under 1 b and such inspection as is found necessary.
   c) 6 inspections per year of the *Central Unit (DSE) of the Police Security Service* (Police Security Service HQ), involving a review of new cases and *the* current *use of concealed coercive measures* (electronic surveillance and mail surveillance), including at least ten random checks in archives and registers at each inspection, and involving a review of all current *cases* (surveillance cases) at least twice a year.
   d) 3 inspections per year of the Defence Security Service (FOST), including a review of the enterprise as a clearance authority, and a review of other security-related activities as found

necessary.

(d)*e*) annual inspection of at least four *police districts* (duty stations in the external surveillance service), at least two *Intelligence Service Units* (duty stations in the local intelligence staff) and/or intelligence/security services at military units and of the personnel security service of at least two ministries/government agencies.

(e) *f)* inspection of measures implemented on its own initiative by the remainder of the police force and by other bodies or institutions that assist the *Police Security Service* (surveillance service).

(f) *g)* other inspection activities indicated by the purpose of the Act."

Section 12 of the EOS instructions

The provisions of Section 12 regulate the Committee's access to comment to the public. In Subsection 1, first sentence, it reads "Commission" instead of Committee, most likely as the result of a typographical error. The Committee proposes that this mistake be rectified (amendments in italics, deletions in parentheses):

"**Section 12.** *Information to the public (Subsection 1)*

Within the framework of the third paragraph of Section 9 of the Act cf. Section 8, paragraph 1, the Committee shall decide what information shall be made public concerning matters on which the Committee (Commission) has commented. When mentioning specific persons, consideration shall be paid to observation of the protection of privacy including persons not issuing complaints. Civil servants shall not be named or in any other way identified except by authority of the Ministry concerned."

5.2. Draft amendments pertaining to the transfer of employment and remuneration authority for the Committee's Secretariat staff from the Presidium of the Storting to the Committee by way of an appointment committee (Section 1, Subsection 3 and Section 14), and amendment pertaining to the matter of security clearance for Committee members (Section 1, Subsection 2)

The EOS instructions contain provisions on the Committee's employment and remuneration authority, in Sections 1 and 14. Section 1, Subsection 3 stipulates that the Presidium of the Storting shall have the authority to appoint Secretariat staff, whereas Section 14, Subsection 2 stipulates that any remuneration to Committee members and Secretariat staff must be determined by the Storting. Since 1996, the authority described in Section 14, Subsection 2 has been vested in the Presidium of the Storting, pursuant to the Recommendations to the Storting no. 157 (1995-96), so that the Presidium is currently responsible for both the appointment of Secretariat staff and determining remuneration to staff and Committee members.

In 2005 the Committee established its own Secretariat, containing staff that were not affiliated with other employers. Wages would from now on be covered by the Committee's budget. The Committee thus took on a more direct responsibility as employer. Currently, the Secretariat has four permanent employees (one administrative clerk, to legal advisers, and one Secretariat Head). Already, this modest number generates quite a few issues concerning appointments, leaves of absence, and remuneration, which burden the Presidium and the Storting's administration.

Since the personnel responsibilities de facto rest with the Committee, and given the recent expansion of the Secretariat, the Committee thinks it does no longer naturally follow that the appointment and remuneration authority for all categories of staff rests with the Presidium.

The Committee proposes, on this basis, that the appointment and remuneration authority for Secretariat staff, with the exception of the Secretariat Head, is delegated to the Committee.

The Secretariat Head is so essential for the Committee that the appointment and remuneration thereof should still be authorised by the Presidium, as is the case for office managers working with the Parliamentary Ombudsman.

Technically, these amendments should be effected on the same pattern as that found in Section 14 of the Act relating to the Parliamentary Ombudsman, i.e. that the actual implementation requires a delegation decision in the Presidium of the Storting, provided that personnel regulations and salary guidelines for the Committee are approved.

The Committee aims to establish provisions in the personnel regulations pertaining to an appointment board, which will be responsible for personnel matters, including issues of remuneration. The Committee presumes that the draft amendments below (where the authority rests with "the Committee") do not preclude transferring the authority to an appointment board, combined with the chance to bring disputes before the Committee, or, if necessary, before the Presidium.

At the same time, the Committee proposes that the provisions in Section 1, Subsection 3 concerning the Presidium making arrangements to find premises for the Committee, together with Section 14, no. 1 regarding Committee costs being covered via the budget of the Storting, be revoked. The Committee has, since its inception, had a separate budget, but this might not have been evident at the time the instructions were established. In any event, the provisions do not represent the current situation and should be revoked. In connection with this, the Committee proposes to move the provisions of Section 14 regarding remuneration to the Committee's members and Secretariat staff to Section 1, so that the issues regarding appointment and wages are dealt with in the same place. Section 14 will then only concern remuneration to individuals called to give testimony or expert statements. Furthermore, the Committee proposes that the authority to determine remuneration for Committee members is vested specifically in the Presidium in the instructions in order to make the instructions more accessible.

In connection with transferring the responsibility for the Committee's accounting from the Storting to the Government Agency for Financial Management (SSØ) in July 2008, the Committee established separate instructions concerning its finance management, which were presented to the Presidium for approval. Transferring the responsibility for accounting entails a more direct administrative responsibility for the Committee, and as a natural consequence thereof, this should also be reflected in the EOS instructions. In light of this, the Committee proposes to include a provision pertaining to the Committee's responsibility for finance management and the development of finance instructions in Section 14, no. 1.

As mentioned in Item 4.2, there is a need to update Section 1 of the EOS instructions in connection with the draft amendments proposed for Section 9, Subsection 2 of the EOS Act. There will thus be a much greater level of correspondence between the EOS Act and the EOS instructions. The proposal requires that the EOS Act's clearance requirements are repeated in the instructions, but this is not deemed to be a problem. In addition, this solution resolves the issue of security clearance for Secretariat staff – which, according to the draft amendments, will still be granted by the NSM.

<u>In light of the above, the Committee proposes that Section 1, Subsection 3, and a new Subsection 4, and Section 14 be amended to read as follows (amendments in italics, deletions in parentheses):</u>

"**Section 1.** *On the Committee and its Secretariat* (The monitory committee)

The Committee shall have seven members including the Chair and Deputy Chair, all elected by the Storting, on the recommendation of Presidium of the Storting, for a period of no more than five years. Steps should be taken to avoid replacing more than four members at the same time.

The members of the Committee shall have security clearance (Those elected shall be cleared) for the highest level of security classification, both nationally and according to treaties to which Norway is a signatory. (After the election, authorisation shall be given in accordance with the clearance)

Remuneration to the Committee's member shall be determined by the Presidium of the Storting. (The Presidium of the Storting appoints one or more secretaries as well as any office assistance, and arranges premises for the Committee and the secretariat. The second paragraph shall apply correspondingly)

The Committee's Secretariat staff shall be appointed by the Presidium of the Storting following a recommendation by the Committee, or, following a Presidium decision to that fact, by the Committee. The same applies to the determination of remuneration to the Secretariat staff. Temporary appointments lasting 6 months or less shall be the responsibility of the Committee. The Presidium shall establish instructions as to the procedures that apply to appointments and the determination of remuneration. The provisions of Subsection 2 shall similarly apply to the Secretariat staff."

"Section 14. (*Costs) Finance management, remuneration to witnesses and experts*

(1. The monitoring costs shall be covered via the Storting's budget.)

(2. Remuneration of the Committee's members and secretariat is fixed by the Storting.)

1. *The Committee shall be responsible for the financial management of the Committee's activities, and separate instructions concerning the Committee's financial management shall be established. These instructions must be approved by the Presidium of the Storting.*

(3)*2.* Any person who is summoned to appear before the Committee has a right to receive compensation for travel expenses according to official rates. Loss of income is compensated according to the rules for witnesses in court cases.

(4)*3.* Experts are remunerated according to the fee regulations for the courts. Higher rates can be . agreed. Other persons engaged to assist the committee are remunerated according to the official scale of fees for committees if nothing else is agreed."

5.3. Draft amendments pertaining to the quorum requirements and the codification of the Committee's access to vesting inspection preparations and the investigation of individual cases in the Secretariat (Section 2)

Section 2 of the EOS instructions stipulates that the Committee is quorate whenever five members are present. Both the requirement that the Committee must have seven members and the requirement that five members must be present for the Committee to be quorate were established on the basis that the Committee needed to secure broad political support for its decisions in controversial cases. However, in recent years, the services and the oversight activities have changed. Oversight today is more administrative in nature, and the large and controversial cases are few and far between. Meanwhile, the Committee has a practical need to be able to reach decisions in matters even though more than two members are absent. In light of this, the Committee proposes to amend Section 2 of the instructions so that the Committee can be quorate whenever four members are present.

This amendment would require the establishment of internal guidelines, stipulating that controversial and principal matters are deferred if fewer than five members are present. In this event, making sure that all members are present for cases like that becomes the

responsibility of the Chair. The Committee presumes that it is unnecessary to codify this in the instructions; it is sufficient that it is included in an internal guideline for the Committee.

In its 2006 annual report, the Committee gave an account of the developments in Committee activities. For example, reference was made to how all inspections of headquarters were prepared by having Secretariat staff meet with the services, carrying out searches of archives and registers and reviewing cases and documents. In its report for 2007, the Committee commented that the day-to-day activities do not allow for a more topical investigation of individual cases and areas. The Committee expressed that there may be a need for such topical investigations in several areas, because these investigations could provide the Committee with a stronger foundation on which to make its assessments. In the draft budget for 2009 the Committee has requested additional resources in order to be able to carry out activities of this kind.

This development entails that an increasing share of the preparatory work prior to inspection is carried by the Secretariat. The shared characteristic of all such activities is that it is supposed to be limited to the collection of data. Internal guidelines have been established in order to secure sufficient documentation of the activities carried out, and to prevent conflict. Central to this issue is that the Secretariat staff always asks, ahead of time, about which types of information they can access, and if the services expresses any reservations, the Committee would have to review the issue of access. The preparatory activities of the Secretariat, as well as its review of individual cases in the services, have been cleared with the services in question.

The Committee is of the opinion that the instructions should be amended to allow for greater flexibility than is the current situation, in terms of the access to transfer preparatory work prior to inspection and other types of data collection to the Secretariat. Such amendments would also entail that the instructions would correspond better to the actual distribution of activities between the Committee and the Secretariat. A development, wherein a larger share of activities is transferred to the Secretariat is necessary, given the timeframes it is realistic to impose on the Committee's members. As far as the Committee is concerned, this is a natural development. As the services have adjusted their activities and established legal frameworks for their activities, some of the oversight activities have become more administrative in nature.

The Intelligence Service has, in a letter of 1 October 2008, raised the issue of Section 5 of the Act, concerning the obligation to appear before the "Committee" if summoned to do so. A copy of the letter is appended hereto. The Committee's assessment is that the proposed instructions must be enforced, with the understanding that the Act of course will supersede the instructions in the event that the issue comes to a head,cf. the account above.

In its letter of 4 November 2008, the Ministry of Defence states that it is by principle sceptical of transferring "oversight functions" ascribed to a quorate Committee to the Secretariat alone or together with one or more of the Committee's members. The Committee emphasises that the tasks proposed delegated to the Secretariat in the draft instructions are associated with preparatory activities primarily concerned with the collection of data, and that the proposal naturally does not plan to transfer any decision-making authorities or process rights to the Secretariat. It follows from documents dating back as far as the Skauge Committee's recommendations that it may become necessary for the Committee to split up or otherwise engage assistance, under the condition that this access is regulated and that the nature of the activity is taken into account, cf. Chapter 4.3. This is how Section 2 of the EOS instructions has been practiced up to this point – in collaboration with the services, as mentioned above.

In its letter, the Ministry further suggests that the instructions should specify that the duty to appear before the Committee does not apply to the Secretariat, when acting alone or

together with individual members of the Committee. The Committee does not have strong hesitations about including this in the instructions, in that it applies to situations in which the Secretariat is acting alone. However, if members of the Committee are present, he or she will always be acting on behalf of the Committee, and the duty to appear if summoned thus applies. This is how this provision has always been practiced. The argument against codifying an exception for the activities of the Secretariat is that it already follows from the EOS Act and instructions, that the individual cannot be ordered to appear before the Secretariat alone. However, if the Storting finds it expedient, it could potentially be included under another item, as a separate point, that the provision obligating summoned individuals to appear before the Committee under Section 5 of the Act does not apply to the Committee's Secretariat when acting alone.

In light of the above, the Committee proposes the following amendments to Section 2 of the EOS instructions, so that it reads as follows (amendments in italics, deletions in parentheses):

"Section 2. *Quorum and working procedures.*

The Committee has a quorum when *4* (five) members are present. The Committee shall as a rule function collectively, but may divide itself during inspection of service locations or installations. .

In connection with especially extensive investigations, the procurement of statements, inspections of premises, etc. may be carried out by *the Secretariat alone or together with one or more members* (the secretary and one or more members). The same applies in cases where such procurement by the full committee would require an excessive amount of work or expense. *Ordinary inspection preparations and reviews of cases at the services may be left to the Secretariat alone.* In connection with hearings, as mentioned in this paragraph, the Committee may engage assistance. (It is then sufficient that the secretary or a single member participates.)

The Committee may also otherwise engage assistance when special expertise is required.

Persons who have previously functioned in the intelligence, surveillance and security services may not be engaged to provide assistance."

6. Collective outline of provisions including draft amendments

To the EOS Act of 3 February 1995 no. 7, the following amendments are made:

Section 1, Subsection 4, new second sentence. Reads as follows:

Within the framework of existing laws and regulations, the Committee shall discharge of its duties autonomously and independently of the Storting.

Section 2, Subsection 1, no. 1. Reads as follows:

The purpose of the monitoring is:

1. to ascertain and prevent any exercise of injustice against any person, and to ensure that the means of intervention employed do not exceed those required under the circumstances, *and to help to ensure that the services respect human rights,*

Section 9, Subsection 2, reads as follows::

The Committee's members and secretariat are bound by regulations concerning the handling of documents, etc., that must be protected for security reasons. They shall be *granted clearance* for the

highest level of security classification, both nationally and according to treaties to which Norway is a signatory. *The Presidium of the Storting shall be the clearance authority for Committee members. The vetting of personnel shall be carried out by the National Security Authority.*

To the EOS instructions of 30 May 1995, the following amendments are made:

Headline of Section 1 reads:
On the Committee and its Secretariat

Section 1, Subsection 2 reads:
The members of the Committee shall have security clearance for the highest level of security classification, both nationally and according to treaties to which Norway is a signatory.

Section 1, Subsection 3 reads:

Remuneration to the Committee's member shall be determined by the Presidium of the Storting.

Section 1, new Subsection 4 reads:

The Committee's Secretariat staff shall be appointed by the Presidium of the Storting following a recommendation by the Committee, or, following a Presidium decision to that fact, by the Committee. The same applies to the determination of remuneration to the Secretariat staff. Temporary appointments lasting 6 months or less shall be the responsibility of the Committee. The Presidium shall establish instructions as to the procedures that apply to appointments and the determination of remuneration. The provisions of Subsection 2 shall similarly apply to the Secretariat staff.

Section 2, Subsection 1 reads:

The Committee has a quorum when *4* members are present.

Section 2, Subsection 2, first sentence reads:

In connection with especially extensive investigations, the procurement of statements, inspections of premises, etc. may be carried out by *the Secretariat alone or together with one or more members.*

Section 2, Subsection 2, new third sentence reads:

Ordinary inspection preparations and reviews of cases at the services may be left to the Secretariat alone.

Section 6, Subsection 1, third sentence reads:

Protests following such decisions may be submitted by *the head of the respective service and the Chief of Defence.*

Section 8, Subsection 2, second sentence reads:

Statements in response to complaints against the *Police Security Service* concerning surveillance activities shall however only declare whether or not the complaint contained valid grounds for criticism.

Section 9, Subsection 2, second sentence reads:

In connection with examinations that may result in criticism of them, the administration's personnel and former employees may also receive the assistance of an elected union representative who has been authorised according to the *Security Act with pertaining instructions.*

Section 11 reads:

1. Responsibilities for inspection are as follows:
   a) For the intelligence service: to ensure that activities are held within the framework of the service's established responsibilities, and that no injustice is done to any person.
   b) For the *National Security Authority:* to ensure that activities are held within the framework of the service's established responsibilities, to monitor clearance matters in relation to persons and enterprises for which clearance *has been denied, revoked, reduced or suspended by the clearance authorities*, and also to ensure that no injustice is done to any person.
   c) For the *Police Security Service*: to monitor *that the service's handling of preventive cases and investigations, its use of concealed coercive measures, its processing of personal data, and the exchange of information with domestic and foreign collaborative partners* is carried out in accordance with current regulations, and meets the requirements for satisfactory routines within the framework of the purpose stated in section 2 of the Act.
   d) For the Defence Security Section: to monitor that the service's execution of personnel security clearance activities and other security clearance activities are kept within the framework of laws and regulations and the service's established responsibilities, and also to ensure that no injustice is done to any person.
   e) For all services: to ensure that the cooperation and exchange of information between the services is held within the framework of service needs *and applicable regulations.*
2. Inspection activities shall at least involve:
   a) half-yearly inspections of the *Intelligence Service*, involving accounts of current activities and such inspection as is found necessary.
   b) quarterly inspections of the *National Security Authority*, involving a review of matters mentioned under 1 b and such inspection as is found necessary.
   c) 6 inspections per year of the *Central Unit (DSE) of the Police Security Service*, involving a review of new cases and *the* current *use of concealed coercive measures*, including at least ten random checks in archives and registers at each inspection, and involving a review of all current *cases* at least twice a year.
   d) 3 inspections per year of the Defence Security Service (FOST), including a review of the enterprise as a clearance authority, and a review of other security-related activities as found necessary.
   e) annual inspection of at least four *police districts*, at least two *Intelligence Service Units* and/or intelligence/security services at military units and of the personnel security service of at least two ministries/government agencies.
   f) inspection of measures implemented on its own initiative by the remainder of the police force and by other bodies or institutions that assist the *Police Security Service*
   g) other inspection activities indicated by the purpose of the Act."

Section 12, Subsection 1, first sentence reads:

Within the framework of the third paragraph of Section 9 of the Act cf. Section 8, paragraph 1, the Committee shall decide what information shall be made public concerning matters on which the *Committee* has commented.

Headline, Section 14, reads:
Finance management, remuneration to witnesses and experts

Section 14, Subsection 1 reads:
The Committee shall be responsible for the financial management of the Committee's activities, and separate instructions concerning the Committee's financial management shall be established. These instructions must be approved by the Presidium of the Storting.

Section 14, current items 3 and 4 become items 2 and 3.

Yours sincerely,

Helga Hernes
Committee Chair

Appendices:
Letter from the Intelligence Service, dated 1 October 2008
Letter from the National Security Authority, dated 9 October 2008
Letter from the Police Security Service, dated 22 October 2008
Letter from the Armed Forces' Security Section, dated 4 November 2008
Letter from Ministry of Defence, dated 4 November 2008
Letter from the Ministry of Defence, dated 3 December 2008
Letter from the Ministry of Justice, dated 2 January 2009