Norwegian Parliamentary Intelligence Oversight Committee

The Norwegian Parliamentary Intelligence Oversight Committee (the EOS Committee)

Annual report 2007

This is an unofficial translation of the report sent to the Storting, Spring 2008

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 the legislation, the issuer of information shall determine what is 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 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.

More detailed information about the Committee and its supervisory activities is included in Appendix 1.

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 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.

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
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. AN OVERVIEW OF THE COMMITTEE'S ACTIVITES IN 2007

1. Main points regarding the inspection of the services

In the Storting's assessment of the Committee's annual report for 2006, the Standing Committee on Scrutiny and Constitutional Affairs requested in their recommendation that the Committee provide more information regarding the follow-up of certain specified issues. An account of these issues is presented in this annual report, with reference to the Committee's request in the relevant paragraphs.

During its oversight of The Police Security Service (PST), the Committee considered a case which related to the registration and deletion concept in the service's intelligence register. The Committee found that intelligence information about people who have been deleted from the register will remain in the register and be searchable on name, providing that the information is linked to other registered people. The Committee has requested that the Service should change its practice or ensure that the regulations are amended so that there is consistency between concept and reality. Upon examination of a joint operation between PST and the Norwegian Intelligence Service (NIS), the Committee pointed out that the current rules for use of methods are not made for joint operations and transfer of responsibility between the services, and it is therefore necessary to look into amending these rules. The examination of the specific operation has not been concluded.

Upon inspection of the personnel security service in the Ministry of Foreign Affairs it transpired that the Ministry did not have appropriate routines for authorisation of its own employees. Moreover, the Ministry had followed a non-conforming practice which was contrary to the rules with regard to the significance of the employees' security clearance when they marry or enter into cohabitation with a person without 10 years' verifiable personal history. During its inspection of the Armed Forces' Security Section (FSA), the Committee looked into a case which concerned the terms for security clearance of personnel in the Armed Forces who are being relocated. The Committee commented on the FSA's apparently passive attitude to the current issues, which according to the available information could be of great significance for the personnel's chances of finding a new position with the Armed Forces.

The above-mentioned joint operation between the Intelligence Service and the PST raised an issue of the same nature with regard to the Intelligence Service, and the Committee has also pointed out to this Service that the regulations are unclear and that it might be necessary to look into the issue of amending the rules. The examination of the specific operation as regards the Intelligence Service has not yet been concluded. As regards the Ministry of

Defence, the Committee found grounds for comments regarding some aspects of the documentation of the operation's political approval process.

2. Inspection activities

Pursuant to Section 11, No. 2 of the EOS Instructions, the Committee's inspection activities shall include at least six inspections per year of the PST HQ, quarterly inspections of the National Security Authority (NSM) and half-yearly inspections of the NIS. Moreover, annual inspections of the PST local units shall be carried out in at least four police districts, of at least two external units in the Intelligence Service and/or intelligence and security service functions at military units and departments and of at least two security clearance authorities outside the NSM.

These regulations have been complied with in the 2007 inspection activities. The Committee carried out a total of 28 inspections in 2007. Of these, six were held in the central unit of the PST (DSE), four in the NSM and three in the central Intelligence Service. Fifteen inspections were carried out of external units of the services, including three inspections of the FSA. The Committee's technical expert has participated in eight of the inspections.

In 2007, the Committee held 20 internal working meetings. A meeting was also held with the Intelligence Service at their central headquarters where some of the Committee members participated.

The following external units and local segments, etc. were inspected in 2007: PST Agder, PST Vest-Oppland, PST Øst-Finnmark, PST Gudbrandsdal, the Ministry of Foreign Affairs, the County Governor of Vest-Agder, FSA Jørstadmoen, the Norwegian Home Guard, the Armed Forces' stations in Fauske and Kirkenes and the Co-ordinating and Advisory Committee for the Intelligence, Surveillance and Security Services (KRU).

3. Complaints and issues raised on the Committee's own initiative

The Committee received 22 complaints in 2007, compared to 16 in 2006. Eighteen of the complaints were directed at the PST, two at the FSA, one at the NSM and one at the Intelligence Service.

During the year, the Committee has raised 18 issues on its own initiative.

4. Meetings and visits

4.1 Meetings with Norwegian authorities

Information meeting at the Norwegian Directorate of Immigration

In the annual report for 2006, the Committee gave an account of the cooperation relations between the PST and the immigration authorities. This cooperation is relatively extensive and information is exchanged on a fairly routine basis between the PST and the immigration authorities regarding visas, asylum applications and deportation cases. The inspection activities necessitate insight into this cooperation. In January 2007, the Committee held an information meeting with the Norwegian Directorate of Immigration. Please see Chapter III, first paragraph, for a more detailed account.

Meeting with the KRU and inspection of KRU's archives

In the 2004 and 2005 annual reports, the Committee stated that the issue of whether the Committee has the right to inspect the KRU archives (the Co-ordinating and Advisory Committee for the Intelligence, Surveillance and Security Services) had been discussed with the Ministry of Justice and the Police on the background of a dispute regarding inspection of one specific document which the KRU had prepared. The case was assessed by the

Ministry's Legislation Department. The Department concluded that the Committee has the right to inspect KRU's work.

In 2007, the Committee held a meeting with the KRU where information was provided on the function and activities of the KRU. An inspection was also carried out of the KRU archives. The Committee was given an introduction into the work of establishing a common understanding and terms of reference regarding the services' threat assessments, the increased need for cooperation between the Intelligence Service and the PST, challenges relating to the exchange of information with foreign, collaborating services and specification of boundaries of responsibility between the services. Information was also given on the specific case which gave rise to the issue regarding inspection of the KRU archives.

The Committee received information about the KRU archives and carried out random checks of these. No issues or circumstances were discovered which would warrant further inspections or follow-up by the Committee. However, it is of principle importance that the Committee has the right to access and inspect KRU's archives.

4.2 Foreign visits, contact with foreign oversight bodies

Meeting with the South African parliamentary oversight committee

In May 2007, the Committee received a visit from members of the South African parliamentary oversight committee; the Joint Standing Committee on Intelligence (JSCI). The committee was established in 1996. In addition to an information meeting with the Committee, meetings were also held with the PST, the Intelligence Service and the NSM, as well as with the two committees at the Storting; the Foreign Affairs Committee and the Standing Committee on Scrutiny and Constitutional Affairs. At the meeting with the Committee, the JSCI was particularly interested in the need to maintain individual legal protection in a situation where the secret services are given increasingly broad authorisations and international intelligence cooperation is increasing.

Seminar in the Hague organised by the Dutch oversight committee for the intelligence and security services

In June 2007, the Chairman of the Committee and the Secretariat attended a conference in the Hague where the topic was international human rights and the accountability of the intelligence and security services. The seminar was organised by the Dutch Review Committee on the Intelligence and Security Services (CTIVD). The conference was attended by representatives from oversight bodies as well as by researchers and human rights experts.

Workshop in Geneva organised by the International Commission of Jurists (ICJ) and Geneva Centre for Democratic Control of Armed Forces (DCAF)

In August 2007, the Chairman of the Committee and the Secretariat participated at a workshop in Geneva. The workshop was jointly organised by the ICJ and DCAF and was attended by both former employees of the intelligence and security services, scientists, judges and human rights lawyers.

In addition to the role of the intelligence and security services and their accountability, the need for further standards and methods of oversight was assessed in view of the technological development and the services' extended authorities following the terrorist threat. At the centre of the discussion were the extent and significance of international human rights. The Chairman of the Committee gave a talk on the Norwegian oversight model with a focus on the challenges faced by the oversight activities concerning the exchange of intelligence information between foreign services, as well as on the technological development.

Meeting with a Polish delegation
In September 2007, the Chairman of the Committee and some of the Committee members held a meeting with a delegation led by the Polish Minister of the Interior Ludwik Wassermann. He is responsible for the reorganisation and democratisation of the secret services in Poland. The Chairman of the Committee gave an account of how the parliamentary oversight of the secret services in Norway is organised. The delegation raised several issues relating to this and was particularly interested in the background for the establishment of the Committee and how the oversight activities were organised in Norway.

Meeting with the Swedish Armed Forces Intelligence Board
In November 2007, the Chairman of the Committee and the Secretariat met with the Chairman of the Armed Forces Intelligence Board (FUN) in Sweden. FUN is a Swedish government-appointed intelligence oversight body. Issues were raised at the meeting relating to the international cooperation between intelligence and security services and the technical challenges of the oversight activities.

Meeting with a parliamentary delegation from Bosnia
In November 2007, some of the Committee members received the Bosnian Joint Security and Intelligence Committee of the BiH Parliamentary Assembly. The visit was initiated by the Norwegian Institute of International Affairs (NUPI), who is running a project in Bosnia for the reform of the intelligence and security services and establishment of a supervisory regime. During the visit, time had been set aside for an information meeting with the Committee concerning the parliamentary control of the intelligence and security services. During the meeting, the Committee was particularly interested in the Norwegian rules for security clearance and the Norwegian Committee's oversight of the same. During the delegation's visit a meeting was also held with the PST, the NSM, the Intelligence Service and the Storting's Committee on Scrutiny and Constitutional Affairs.

Meeting with the Swedish Commission on Security and Integrity Protection
In November 2007, the Committee's secretariat received the Chairman of the Secretariat and office manager of the Commission on Security and Integrity Protection (SIN) in Sweden. The Commission is a newly-established oversight body, which only becomes operative in 2008. The purpose of their visit was to obtain information about the Committee's administrative routines relating to meetings, inspections and document handling.

The Commission on Security and Integrity Protection will perform an oversight of the Swedish police security service, SÄPO, which is similar to the EOS Committee's oversight of the PST. The visit provided useful input for the work of our Committee as well. These kinds of contacts are very important for the exchange of information about oversight activities. This is particularly true for oversight bodies with clear similarities to the Committee. Contact will be maintained with the Commission on Security and Integrity Protection in the future.

Meeting with the Canadian oversight body
In November 2007, the Secretariat visited the Canadian oversight body SIRC (Security and Intelligence Review Committee). SIRC is an independent oversight body for the Canadian security and intelligence service (CSIS) and reports to the Canadian parliament. SIRC was established in 1984 and has broad experience. Their oversight activities are to a large extent comparable to the oversight activities of the Norwegian Committee.
The purpose of the visit was to acquire information about and a practical introduction into the work methods the Canadians employ in their oversight activities and to hear their assessment of these methods. SIRC's work is to a large extent project-based and the meeting gave the Secretariat a useful introduction into such a work process, describing the criteria for the selection of project topics and planning of each project, the relationship between the Secretariat and the Committee regarding project implementation and showing

how the projects are presented to the Committee and in the Committee's annual report. Project work as a work method is described in more detail in Chapter VI, paragraph 3.

III. NORWEGIAN POLICE SECURITY SERVICE (PST)

1. Inspection, in general about the supervision of the Service

In 2007, the Committee carried out six inspections in the Central Unit (DSE). Inspections were also carried out of the local PST units in Agder, Vest-Oppland, Øst-Finnmark and Gudbrandsdal.

In 2007, the Committee received 18 complaints directed against the PST from private individuals, compared with 14 in 2006. All complaints have been investigated centrally in the DSE and locally where the Committee found it appropriate. A complaint which was directed against the PST and which the Committee concluded in 2007 was also investigated by the ordinary police, on the basis of the complainant's submissions. There were no grounds for criticism in any of the cases.

In the 2006 report, the Committee described the significance of the requirements concerning specific assessment stipulated in the Security Act and the Freedom of Information Act when an application for disclosure of information is submitted to the PST. These provisions apply to the PST even if the Service's journals and documents are basically exempt from public disclosure in their entirety pursuant to the Regulations relating to the Freedom of Information Act and are regularly classified pursuant to the Security Act. The Committee has found it necessary to look into these regulations and how the Service implements them in more detail. The reason for this is that the Committee receives a number of requests from people whose applications to the PST for access have been denied, and in some of the complaint cases the right to access is also a topic. In 2007, in conjunction with a specific complaint case, the Committee therefore discussed with the PST and later with the Ministry of Justice and the Policehow the provisions in the Freedom of Information Act and the Security Act relating to increased access and requests for de-classification are understood and put into practice.
The Committee will continue its assessment of these issues in 2008.

On the basis of the Committee's spot checks of PST's intelligence register, the Committee raised some fundamental questions in 2007 concerning the Service's handling of personal data in the register. One important question in this case has been whether the requirements laid down in the PST regulations and in the Service's guidelines for handling of personal data apply to all forms of registrations in the mentioned register. Another important question concerned PST's routines for deleting information from the intelligence register. More details concerning this issue are provided in section 3 below.

In its 2005 annual report, the Committee stated that it would put more emphasis on acquiring knowledge about the cooperative relationships between the security and intelligence services and other public authorities because of the significance such knowledge about relations and interfaces may have for the oversight of the services. There might also be a direct inspection responsibility vis-à-vis the authorities that cooperate and exchange information with the services. In this connection, reference is made to the Committees' area of oversight being functionally defined which, pursuant to the provision in Section 11, No 2, letter e of the EOS Instructions, also comprises other bodies or institutions that assist the PST.

As part of this work, the Committee met with the Norwegian Directorate of Immigration (UDI) in 2007. At the meeting with the Directorate, the Committee was given further information about the activities in general and about the collaboration with the PST. The management of the Directorate and the PST management meet on a regular basis to discuss issues arising from the collaboration. The Directorate stated that work is ongoing to formalise the

collaboration to a greater extent through, among other measures, written guidelines for the exchange of information and contact.

The UDI emphasised that they will assess a case in accordance with the Immigration Act even if the PST has provided information in the case. The PST assessment or recommendation can, however, still be significant within the discretionary margin that the Directorate has pursuant to the Act. Pursuant to Section 38 of the Immigration Act, the Ministry of Labour and Social Inclusion also has the right to make use of its instruction authority if the Ministry is of the opinion that classified information from the PST calls for a certain outcome or specific procedure.

The Committee will look into the exchange of information between the PST and the UDI in more detail.

2. Inspection of archives and registers

2.1 Introduction

The inspection of archives and registers is a central part of the Committees' inspection activities in the PST. The Committee's task is primarily to prevent unlawful handling of personal data and to ensure that information which is no longer necessary or relevant is deleted.

For each inspection, the Committee carries out random checks of the Service's electronic intelligence register and of its administrative procedure and record-keeping. The inspection of the archives and registers is prepared by the Secretariat who will carries out different types of searches and spot checks prior to each inspection.

Also in 2007 the Committee carried out regular random checks of the registrations of personal information that were maintained after the five-year evaluation. The Committee checks that the deadline for reassessment is kept, how the discretionary exclusionary provision is put into practice and that the reason for the continuation is apparent from the register. The consequence of the continuation is that the registrated information will remain in the register for another five years.

The most important points of oversight as regards registrations of personal information are whether a specific and individual assessment has been made, both of the quality of the available information and its professional relevance. The Committee considers whether the reasons presented and the actual information upon which the registration is based meet the requirements in the PST directive concerning the purpose, necessity and quality. As will be seen below, the guidelines for handling of information in the PST ensure that the Committee now has more specific requirements for the handling of information that they can assess the PST archives and registers up against.

In 2007, the Committee discussed several individual registrations with the Service. Questions were raised concerning both the basis for the registration and the continuation after five years. In some cases, the Service reassessed and deleted the registration. In other cases the basis for the registration was clarified as a result of the inspection, so that the Committee had no grounds for criticism.

2.2 Repeal of the Disclosure Act and shredding stop for PST

The Access Reviewing Committee was appointed by Royal Decree on 22 December 1999 to process applications for disclosure and compensation pursuant to the Provisional Act of 17 December 1999, No. 73 concerning limited access to the archives and databases of the Secret Police Service (the former name of PST), also known as the Disclosure Act. Private individuals were given the possibility to submit an application to access information about

themselves for the period 8 May 1945 to 8 May 1996. The application period extended from 1 January 2000 to 31 December 2002.

The Access Reviewing Committee and the Complaints Commission for the handling of complaints regarding the Access Reviewing Committees' decisions concluded their work in 2007 and submitted their final reports to the Ministry of Justice and the Police on 15 January 2008. The Disclosure Act was repealed with effect from 31 December 2007. The Access Reviewing Committee's archives have been transferred to the National Archives of Norway.

On 26 June 2007, the Ministry of Justice and the Police abolished the shredding stop for PST, which applied to documents registered in the Service for the period 8 May 1945 to 8 May 1996 and which was upheld on the grounds of the Access Reviewing Committee's work. The Ministry states that the archive material in the PST for this period has been reviewed by the Service so that the material can now be transferred to the National Archives of Norway, unless there are official reasons for the material to be kept with the PST. The Service has stated that work is ongoing to transfer the documents from the PST to the National Archives. The Ministry assumes that routines will be established which will secure the PST, the Ministry or the Committee access to the documents if necessary.

2.3 Internal guidelines for the handling of information in the PST

Chapter IV of the Code of Practice concerning the Norwegian Police Security Service (the PST Code of Practice) laid down by Royal Decree on 19 August 2005, stipulates overall rules and requirements for the handling of information by the Service. Section 16, second subsection, of the Code of Practice stipulates that the Service must draw up more detailed guidelines for the handling of information. These must be approved by the Ministry of Justice and the Police.

In its 2006 report, the Committee stated that the compilation of the guidelines, which are to give supplementary provisions to the 2005 PST Code of Practice, has taken longer than expected. The PST submitted their draft to the Ministry of Justice and the Police for approval in November 2006. The guidelines were not approved by the Ministry until 12 December 2007.

Pursuant to Section 16, first subsection of the PST Code of Practice, the guidelines shall be supplemented by an internal control system in the PST. Chapter 6 of the guidelines stipulates further provisions regarding the content of the internal control. The PST has informed the Committee that the internal control system is under development.

Pursuant to Section 1-1, the guidelines apply to the handling of information by the PST when the Service is performing its preventative tasks under the provisions of the Police Act and for the Service's handling of information in connection with immigration control and vetting. Handling of information during PST criminal investigations is excluded. This is regulated by the provisions in the Criminal Procedure Act and the Prosecution Instructions.

As in the PST Code of Practice, the same terminology is used in the guidelines as in the Personal Data Act. Thus the requirements in the guidelines are linked to the phrase: "processing of personal data"; a broadly defined phrase which includes any electronic or manual handling of information. A "registration in the intelligence register" is in Section 1-2, No. 7 defined as "the processing of personal data deemed necessary for the PST to solve its tasks and which does not qualify for establishment of or incorporation into a preventative case."

Quite specific requirements are laid down in Chapters 2 and 3 of the Guidelines concerning the purpose, necessity and relevance of the information that is to be processed. Section 2-1

specifies that the purpose of the information processing must be specified in detail when a preventative case or registration in the intelligence register is established. In the provision relating to what categories of people information can be processed about (Section 3-2) a requirement has been laid down stipulating that the individual should be labelled with the role he or she has as a registered person in the intelligence register, something which will give an indication of whether the processing of the personal data should be regarded as being of a positive or negative character. For registrations it is also a requirement during the initial processing that a specific work hypothesis is formulated where the professional assessment relating to the requirements for purpose, necessity and relevance must be stated, cf. Section 3-4.

Information processed by the PST must not be kept any longer than necessary for the purpose of the processing, cf. Section 3-7. The rule stipulated in the previous registration circular concerning the review of registrations where no new information has been added after five years, is upheld herein. The data must be deleted if they no longer serve a purpose. The guidelines also introduce the term “blocking” which is given as an alternative for information which should not be deleted for reasons of notoriety, but that should instead by kept at the National Archives.

Chapter 4 of the Guidelines on disclosure of information is discussed in more details in Section 4 below regarding the disclosure of personal data to foreign cooperating services.

The Guidelines for the processing of information in the PST ensure a strengthening of the rules for this very important function of the PST activities. The Service’s intelligence register is extensive and contains a large amount of sensitive personal data. A coordinated regulatory framework for the use of it is therefore of great significance.

2.4 The Service’s compliance with the requirement for individual assessment prior to registration

In 2007, the Committee questioned several individual registrations on the basis of its spot check findings. The Committee has pointed out that the information in some of the registrations was not sufficient to be able to assess the registration’s relevance to the PST’s tasks. In others, the Service should have followed up a registration more closely in order to clarify, for instance, any affiliation with an environment or an organisation. As regards evaluation of registrations which have been kept for five years without new information being added, the Committee has had grounds for criticism regarding the reasons why a registration is maintained in quite a great number of cases. An issue which arises frequently relates to the assessment requirements when a person is registered exclusively because of his or her affiliation with another person. The question here is often whether the affiliation in itself can be regarded as sufficient. During 2007, the Service has deleted or amended information about approximately 20 people from its register as a consequence of the Committee’s questions following spot checks.

As stated in previous annual reports, the requirement relating to an individual assessment prior to the Service’s processing of information about individuals is a prioritised control area. In connection with the processing of the Committee’s annual report, the Committee has emphasised that this is an important area. An individual assessment must be carried out by the Service in order to comply with the requirements for purpose, necessity and relevance pursuant to the PST Code of Practice and the new guidelines. It appears that the new guidelines might make the requirements even more stringent, due to the stipulated requirements concerning a specific statement of the purpose of the processing and the requirement relating to the formulation of a specific work hypothesis the first time a registration is processed, cf. Section 2-1 and 3-4 of the Guidelines.

The Committee's general impression of PST's processing of information in the intelligence register is that the PST is working to achieve a common understanding of the regulations and that the "thresholds" that should apply in the processing of information about private individuals in the intelligence register are fairly uniform throughout the service. There is reason to believe that the new guidelines for the Service's processing of information will promote this further.

2.5 Inspection of topical archives and archives of personal records
Also in 2007 the Committee has inspected topical archives and archives of personal records in the PST. In this connection, the focus of the inspections was to check that the Service had reviewed and set aside cases and documents with no professional relevance and that reviewed documents that had been prepared for shredding or hand-over were being kept separate from other archive material. The Committee did not reveal any shortcomings in this area for 2007.

As the shredding stop for PST has been abolished, the Service must now, both centrally and in each police district, hand in irrelevant material to the National Archives. The Committee will keep itself informed about the Service's work on this in 2008.

2.6 Local intelligence registers
In the light of the PST establishment of a common intelligence register in March 2005 which implied abolishment of all former manual and electronic intelligence registers in the PST, the Committee has paid close attention to this, particularly when inspecting the local districts. The Committee has previously reported that in some places the abolishment of the local registers has taken a long time.

Also in 2007, the Committee discovered a local intelligence register during an inspection of a local PST unit. The Committee raised the issue with the DSE. In their reply to the Committee, the DSE regretted that the unit had not yet abolished the register. The DSE informed the Committee that after the introduction of the intelligence register SMART in 2005, guidelines were provided for the police districts regarding a review of the local intelligence registers with a view to transferring relevant information to SMART and setting aside the remaining documents for shredding/hand-over. DSE informed the Committee that they had raised the issue with the district in question.

3. The concept of registration and deletion in PST's intelligence register

In 2007, the Committee wrote to the DSE concerning two issues which related to the processing of information in the Service's intelligence register SMART. One of the two questions the Committee had was whether the requirement relating to a specific assessment of necessity, purpose and relevance, etc. stipulated in Sections 13-15 of the PST Code of Practice also applies to people who are mentioned in the intelligence register, but who are not registered as objects. The reason for the question was that also people who are only mentioned in the register are easily searchable. The Service had the following reply:

> "As the Committee is aware of, the registration term is incorporated into the broader phrase "processing of personal data" in Section 12 of the PST Code of Practice. This is consistent with the traditional personal information protection legislation, cf. Section 2, No. 2 of the Personal Data Act. The quality requirements related to the processing of personal data in Sections 13 to 15 of the Code of Practice are thus linked to the processing of personal data in their entirety."

In the light of the Service's definite clarification that the requirements relating to quality and relevance, etc. apply to all personal data in the register, this did not give grounds for further follow-up from the Committee.

The other question that was raised related to the concept of deletion in SMART. The central question was whether the distinguishing in SMART between objects and persons mentioned also meant that only people who were registered as objects were comprised by the current regulations on evaluation and potential deletion after five years. The background for this was that it was revealed during spot check searches on deleted objects in the intelligence register that there had been cases where the person was still registered with the same intelligence information. In their reply the PST stated:

> **”Persons mentioned in the free text of an incident**
> The Committee points out that it seems that deleted objects still appear in the register, not as objects, but as ”affiliated”.
>
> The PST would like to briefly clarify the use of concepts as regards affiliation. As a general rule, all objects mentioned in an incident must be linked (”affiliated”) to the incident through their role. The reason for the use of roles is that it is desirable to show what type of affiliation the object has to the incident. This will make it easier to make use of the information in, for instance, analyses. The objects are assigned roles such as main object, mentioned, witness, contact, etc. If we understand the Committee correctly, the concern relates to those objects where the Service regards the information to no longer have a purpose, relevance or necessity for the Service and which should therefore be deleted. Primarily, the concern is directed towards those persons who are mentioned in free text in an incident which will remain in the register and who consequently will appear in free text even though the person has been deleted as an object.
>
> The group of people focused on by the Committee will be excluded from the 5-year re-evaluation lists. The current system does not open for the possibility of removing people who are only mentioned in the free text of an incident. Quality-assuring the entered incident is therefore important. That a person is mentioned in the text of an incident may be significant for the content of the incident, even if the person as an object is no longer regarded as relevant for the Service and is therefore deleted. As long as the incident is relevant for another object, which is must be for it not to be deleted, we find it relevant to keep the name in order to gain a complete picture of the incident. If the name cannot be kept in an incident there is a risk of ending up with a situation where the incident loses much of its value also for the/those remaining object(s) linked to the incident.
>
> It is an objective of the Service to avoid unnecessary personal data from being retained in SMART. The use of free text searches in the incident has not been facilitated in the system’s user plan. Nor would it in the Service’s interest to enter relevant objects as persons in free text, as one would lose much of the functionality the system has been developed for.
>
> As regards objects that are deleted in accordance with the four months’ rule, but where the person is also mentioned in the free text of an incident, we believe that as long as the incident has been quality-assured and thus deemed to be relevant, there should be an opening for this, cf. the above.
>
> **General**
> The very fact that we are working in an intelligence system means that some personal data will be found in the free text field for incidents. To gain a complete picture of the incident in question, it may be relevant to include some personal data in the incident even though creating a separate object for the person may not be relevant for the Service. It is only after all objects relating to the incident are deleted in accordance with the five-year rule that the incident and its content are regarded as irrelevant and should be deleted. In this way, one can ensure that personal data are not kept unless they are relevant to the Service.
>
> As regards registrations in SMART, the PST believes it is important to distinguish between positive and negative registrations. Positive registrations mean registrations where no encumbrances are associated with the person/object. It may be persons who are sources, who have reported something, etc. In some cases, the PST will need to register these persons, but also here on the basis of an assessment of relevance. In some cases it will be

necessary to mention persons in the free text of an incidence, as it will be significant for the police's professional assessment of relevance relating to the incident in question. As long as the person is only mentioned in the free text the Service does not regard such a person as negatively encumbered. In this connection, it should be pointed out that the distinction between positive and negative registrations is not new. The distinction also existed under the NCR[1] and was accepted then."

In its final letter to the Service, the Committee had the following comments:

> "Section 12, No. 1 of the PST Code of Practice gives a very broad definition of the expression "processing of personal data". This comprises any gathering, keeping and communication of information, including registration. Pursuant to Section 13. No.i, letter b), the Service can only process information when necessary for the execution of their tasks and according to Section 14, first subsection, No. 3, the Service is not entitled to "save" (i.e. process) the information for any period of time longer than what is "necessary for the purpose of the processing". No other rules have been laid down in the Code of Practice with regard to storage time and deletions. However, such regulations have been stipulated in the new guidelines (which at this time we understand will replace the former registration circular for the PST).
>
> Contrary to the Code of Practice, the Guidelines employ the term registration. In Section 1-2, No. 7 of the Guidelines a registration is defined as the "the processing of personal data deemed necessary for the PST to solve it tasks and which does not qualify for establishment of or incorporation into a preventative case." As regards contents, this definition seems to be the same as the description of the fundamental necessity criterion in the said provision in Section 13, No. 1, letter b of the Code of Practice. Section 3-7 of the Guidelines lays down rules regarding deletion. The third subsection of the provision reads: "(W)ork registrations where no new information has been added after five years must be reviewed. The data must be deleted if they no longer serve a purpose."
>
> It is difficult to see that the wording in these rules jointly give the opportunity to keep intelligence information about a person after he or she has been deleted as an object, even if the purpose will be different after the object has been deleted – namely to maintain the context and meaning of incidents that are still of professional relevance. If the Service is of the opinion that there still are professional reasons for keeping the information (even for other reasons than to monitor that person in particular), it is in fact implied that the information should not be deleted. If the term "registration" is to be interpreted as the object part of a registration, as opposed to the affiliated incident information, it would, according to Section 3-7, third subsection, be possible to keep the incident information. However, the definition does not indicate that that has been the intention, nor does such an interpretation seem to reflect the referenced provisions in the PST Code of Practice.
>
> To illustrate the Committee's understanding of the practice we take as an example that if A has been registered due to participation in a violent demonstration, his personal data of various types and the registration category/role will appear as object information, whereas the description of the basis for the registration will be incident information. If A is deleted as an object the fact that he has been an object will be removed from the register. However, if the organiser of the demonstration is registered as an object and is linked to the same incident (the description of A's participation in the demonstration), that information will remain in the register until the organiser has been deleted.
>
> In other words, the way the deletion routines for SMART have been organised, information about a person who has been deleted as an object will still appear in all incidents where the person's name is mentioned, as long as there are still other objects linked to the incident. The information will be easily retrievable by searching in incidents in SMART and may be stored for a long time if other objects related to the same incident continue to be of interest to the Service. Consequently, negative information about a person will in many cases exist in SMART even after the Service has concluded that there is no longer a professional basis for maintaining the registrations on the person in question.

[1] NCR was the name of PST's former intelligence register.

On the basis of this, the Committee recommends that the Service reviews the issues that have been pointed out and makes any necessary changes to the practice or regulations. It must be emphasised that the Committee appreciates that the police might have professional reasons for wanting to keep incidents unchanged if a partial deletion or anonymising would compromise the contained meaning. It is, however, of great significance to the Committee's oversight activities and reporting that there is congruence between regulations and practice and between terms of reference and reality.

Finally under this section, some remarks must be made concerning a somewhat different category of registered persons. This concerns persons who have never been registered as objects in SMART, but who are only mentioned in the entry in the free texts relating to incidents. With the Service's current practice, this category will never be assessed for deletion. Here there might be a risk of evasion as it might be tempting to register information about a person in free text (incidents) without creating separate objects for them, in order to avoid the deletion routines.

PST informs the Committee that the Service does not attach anything negative to this category – if that were the case, they would be registered as objects. In this connection it must be pointed out that if a person is not registered as a separate object in SMART, there will be no role specification under the current system indicating whether the registration is positive or negative. (It is currently unclear whether this will be amended in and by Section 3-2 of the Guidelines). Furthermore, the Committee has seen examples of registrations of a negative nature without the person in question being registered as an object. Nor is it always easy to determine if for instance a connection is of a negative nature. In the main, however, when it comes to this category it will naturally not be a matter of direct negative or incriminating information.

The equivalent issues relating to the relationship between regulations and practice as described in the above also apply for this category."

The Committee has requested a reply from the Service.

4. Disclosure of personal data to foreign collaborating services

The Committee has continued the practice of carrying out regular spot checks of DSE's disclosure of personal data to foreign collaborating services in 2007. The established inspection routine entails that the Service at each inspection presents an overview of what has been disclosed since the last inspection. Random checks are carried out of the overview where the Committee requests to see all case papers which illustrate the reason for the disclosure. In 2007, the Committee also carried out spot checks by searching on disclosed information which had been entered in the Service's electronic record-keeping system.

The random checks carried out in 2007 did not reveal any grounds for criticism of the Service. The Committee's impression is that the amount of disclosed information is still increasing. In particular, this seems to be the case for the bilateral exchange of information. The Service also states that it is aware of the negative consequence the disclosure of information may have for, for instance, families in the home country and generally speaking the Service exercises caution both with regard to what type of information is disclosed and to whom. As explained earlier, the Committee's inspection opportunities are limited due to the fact that in many cases the extent of information is sparse, at the same time as the conditions for disclosure often are discretionary. However, the latter seems to have changed somewhat in the new guidelines discussed below. In this connection it must be added that in individual cases where the Committee has requested detailed information, the Service has provided as much information as possible.

In Chapter 4 of the above-mentioned Guidelines for the processing of information in PST, provisions have been laid down regarding disclosure of information from the Service. Section

4-1 reads as follows regarding disclosure of information to collaborating partners in other countries:

> ”Information can be disclosed to foreign collaborating police authorities and to security or intelligence services to avert or prevent criminal acts or if it is necessary for the verification of information. Such disclosure must, however, only take place subsequent to an assessment of the proportionality between the purpose of the disclosure and the consequence this has for the individual.”

The Guidelines introduce a definite requirement for proportionality between the purpose of the disclosure and the consequence for the person in question. Moreover, the provision stipulates that in their assessment of whether the information can be disclosed, the PST must focus on the quality and importance of the information, who the information is about and who is the recipient of the information. Unverified information can only be disclosed if required for important security-related reasons. Furthermore, it must be stated that the information is unverified. Pursuant to Section 4-2, the PST must keep a record of disclosed information, including what type of information has been disclosed, who is recipient of the information and why the information has been disclosed.

The conditions for disclosure of information from the PST to collaborating services have not previously been set down in writing. However, the PST has informed the Committee that up until now the practice has been in accordance with the requirements formulated in the Guidelines. The new regulations are also of a somewhat discretionary character. However, a requirement relating to proportionality has been stipulated and the assessment must take several listed and specific elements into account. It is to be assumed that the regulations will facilitate a better external control.

5. PST’s use of concealed coercive measures

In its 2006 report, the Committee accounted for its oversight of the PST’s use of concealed coercive measures. The PST has access to the same concealed coercive measures as the rest of the police service. Typically, these include communication surveillance, electronic room surveillance, ransacking, etc. As a result of the amendments made to the Criminal Procedure Act and the Police Act which entered into force in 2005, the PST was, as the rest of the police service, allowed to make use of coercive measures during investigations to avert criminal acts – not just to solve them, as was the case previously. Furthermore, the PST was, as the only police authority, granted permission to employ coercive measures outside of an investigation to *prevent* criminal acts.

The Committee has also in 2007 overseen the use of coercive measures in individual cases. One of the aspects of the control is to inspect the Service’s total information basis for individual cases in order to check congruence between this and the request to the court. Another important control point is to ensure that the PST’s use of the coercive measure is in accordance with the court’s permission – typically that a coercive measure is not used beyond the time specified by the court. It is also checked that the measure is terminated if the conditions for the use are no longer present, i.e. if the suspicion or investigation basis is disproven. The total use of coercive measures will also constitute one of the Committee’s control points.

In their preparation of the draft legislation the Storting stipulated that the statutory authority to employ coercive measures for *preventative* purposes was to function as a very limited supplement and a narrow safety valve for the PST, reserved for the prevention of the most serious illegal acts such as terrorism. A further condition was that the Service must always choose the investigative method if possible. Moreover, the Storting also stipulated in their preparation of the draft legislation that the EOS Committee pay special attention to the Service’s use of the new coercive measures.

The 2007 inspection of the Service's use of coercive measures in individual cases has not revealed grounds for criticism of the PST. However, the Committee did notice an increase in the Service's use of their new authority, though this is still moderate. This increase applies to the use of coercive measures for preventative purposes in particular. It is especially in the use of methods such as wiretapping and electronic room surveillance that there has been a distinct increase in preventative cases. Simultaneously, there has been a slight reduction in the use of these methods in investigation cases.

The Committee assumes that the reason for this development is connected to the fact that the Service is more conscious of establishing a preventative case rather than an investigative case when the Service in practice is involved in prevention. Drawing the line between averting investigation and prevention can be difficult, both in a legal and actual sense. It is important for the Committee to check that the Service does not launch an investigation using coercive measures for the purpose of aversion in cases that really are of a preventative character. On the basis of the condition that the use of coercive measures for preventative purposes must be employed with great caution, the Committee will still monitor the Service's choice of method. As the use of coercive measures in preventative cases requires a weaker investigative basis, the Committee will also supervise the Service to ensure that intrusive coercive measures are only employed to prevent the most serious illegal acts, in accordance with the Storting's stipulation. Whether the information presented to the court provides a fair picture of the case is an important control point in this connection.

An inspection of the PST's use of concealed coercive measures is challenging and requires the Committee to go into individual cases in great detail. Furthermore, the Committee's subsequent inspection to ensure that there is congruence between the Service's total information material and the request to the court is particularly resource-demanding. Thus this can only be done to a limited degree during the ongoing inspection activities. The Committee will assess whether a more thorough inspection of a selection of completed individual cases in a project would be a more appropriate control form. Cf. the discussion of such a work method in Chapter VI, Section 3.

6. Joint operation between the PST and the Intelligence Service

In 2007, the Committee inspected one joint operation by the PST and the Intelligence Service. As part of the inspection, questions were raised relating to the application of criminal procedural coercive measures in such a connection and, more generally, about what rules should be applied and what perspectives should be established for the transfer of responsibility and information-sharing in joint operations involving the use of methods.

The specific operation is still being examined and will not be discussed in more detailed here. However, the inquiries that have already been carried out show that it is necessary to look into the regulatory situation regarding joint operations in more detail, particularly when it comes to the use of methods. At a meeting with the PST, the Committee expressed the necessity of this and pointed out that the current situation is not satisfactory.

In the Committee's view a review and evaluation should be initiated of the set of rules that are relevant to and that may become applicable for this type of collaboration. The situation will often be that obvious efficiency considerations related to the safeguarding of national security interests conflict with the safeguarding of the individual's legal protection. To the extent possible the balancing between such considerations should be clarified in an act or other regulations and not be left to open interpretation. Pursuant to the EOS Act, the Committee must have the individual's legal protection in mind. In a situation where the regulations are unclear, it is the Committee's responsibility to question the use of methods that invade the individual's private life. This responsibility must be taken seriously by the

Committee even if it might cause disagreement with the services. The Committee wishes to specify that this is what constitutes the oversight responsibility. However, it must also be said that our current relationship and communication with the Service is by no means problematic.

The Cooperation Regulations for the Intelligence Service and the PST (stipulated by Royal Decree of 13 October 2006) have facilitated increased cooperation and exchange of information between the services. Pursuant to Section 1, this is also an expressed purpose of the Regulations. The Regulations specify that each of the services must operate within the framework of its own legal authority. As the legal authority has been formulated it is in practice not always easy to draw a clear line in a joint operation.

7. The cooperation between the PST and the Intelligence Service

In its annual report for 2006, the Committee describes a case which relates to the cooperation between the PST and the customs authorities. The Committee had raised certain questions with the Directorate of Customs and Excise relating to the checking of the legal basis for the cooperation. Questions were also raised concerning two specific customs checks which the custom authorities had carried out on request from the PST.

The Directorate stated that the customs authorities do not have legal authority to carry out customs checks outside the “custom administration area”. This entails that the customs authorities will independently assess whether there is legal authority when there is a request for assistance from the PST. The Directorate informed the Committee that there are no written guidelines for the cooperation with the PST or the rest of the police service, but that a work group had been established to assess the need for this.

As regards the two specific customs checks, the Directorate reported that it was not possible in retrospect to see what information provided by the PST had proved the reason for carrying out the controls. This lack of notoriety was criticised by the Committee who at the same time gave notice that the reason for the controls will be examined further in the PST.

In 2007, the Committee followed up the case by examining the basis for the two requests for customs checks made by the PST. In one of the cases it emerged that the PST had not provided any detailed information about the case, but that the custom authorities had received it as a ”tip”. As nothing emerged during the review of the case documents in the PST indicating that the PST’s basis for suspicion was related to the customs legislation, the Committee requested a more detailed specification of the background for the tip. The PST replied that the person whom the tip concerned was related to the PST’s main suspect in a case concerning suspected preparation of a terrorist act abroad and that travel had been organised to the country where the alleged terrorist act was to take place. The PST was of the opinion that the person in question could have objects in his luggage which might be used to carry out the act.

At the closure of the case, the Committee drew attention to the fact that it was only in retrospect that the Service had specified a basis for suspicion relating to the customs legislation. The Committee pointed out that even when information was eventually provided, it was not very specific – as regards the customs legislation. The Committee also stated:

> ”In the Committee’s view the fundamental question is, what requirements should be set regarding specific grounds for suspicion. If, for instance, family relations to or friendship with a person under PST’s preventative scrutiny due to suspected terrorist connections are deemed sufficient in themselves, it will in fact give the PST permission to extrajudicial ransacking of a great number of people, even if it is only in connection with border crossings. It would be difficult to oversee such a practice as the criteria would be very vague. The fact that ransacking, particularly of a person, infringes the integrity of the person warrants a clearer

> system which is easier to inspect. The same applies to the fact that the PST must have a court order to carry out such measures in all other contexts.
>
> It is correct as the PST points out that the customs service is given very broad and discretionary access to exercise their control, pursuant to Section 12 of the Customs Act. However, the provision stipulates certain requirements as the customs control must ascertain whether there has been evasion of customs control in respect of any goods or whether an attempt has been made to evade such control. There is a prerequisite herein that there must be indications that one is within the custom administration area, and a tip from the police should to a certain extent be specified in such a case. As the Committee has pointed out previously, it is in this connection a point that a tip or request from the PST would normally carry great authority. This places a responsibility on the Service."

Regarding the inspection of the other customs control, it emerged that the PST had obtained a court order for a secret search of the suspect's luggage. However it also emerged from a customs memo, available at the PST, that the customs control which was conducted was more extensive than authorised by the court order. In reply to the Committee's query, the PST stated that prior to the customs control a meeting was held between the PST and the customs service where the court order for a secret search of the luggage was presented. The custom services also received a copy of the order. Consequently, the PST regarded the information about the limitations of the court order as having been made available to the customs service.

In reply to the Committee's query, the Directorate of Customs and Excise stated that the customs control was exclusively prompted by the PST's request and that there were no other customs-related indications prompting the customs control. Consequently, the Directorate acknowledged that the control should not have exceeded the limits of the court order and regretted that the people in question had been subjected to an extended customs control. Furthermore, the Directorate stated that during the last year special attention had been paid to the issues raised by the Committee and that the custom regions had been made particularly aware of the fact that: "one should not exceed the control measure mandate which the requesting authorities must relate to."

On the basis of the Directorate's account, the Committee had no further comments to that specific customs control.

In their review of the 2006 annual report, the Standing Committee on Scrutiny and Constitutional Affairs asked the Committee to follow up the efforts of drawing up guidelines and to report back on the issue. The Committee has received information about this work through inspections in the DSE in 2007. The Committee has also raised the issue with the Directorate of Customs and Excise. The Directorate reported that on 24 January 2008, a cooperation agreement was signed between the PST and the Directorate which stipulates that the cooperation and exchange of information must take place within the parties' statutory basis and that notoriety must exist regarding the exchange of information. However, new guidelines have not yet been prepared. In its conclusion of the cases accounted for in this report, the Committee emphasised to both the PST and the Directorate the importance of drawing up more detailed guidelines for the operative cooperation.

8. Procedures for entries on and deletions from the UN terror list

Since 2001 the UN has, through a special regime administered by the UN Committee of Sanctions, kept a list of persons and organisations that belong to or are affiliated with the Taliban or Al-Qaida. Being listed by the UN Committee of Sanctions may have serious consequences for the individual as listings entail a binding commitment for all UN member countries to freeze financial assets belonging to the person or organisation in question, as well as the imposition of travel restrictions. Criticism has been raised relating to both entries on and deletions from the list, especially due to the lack of opportunity for having entry

decisions heard by a court. The Ministry of Foreign Affairs is responsible for implementing the national obligations arising from such listings. During an inspection of the KRU in 2007, the Committee was informed that work is ongoing to review what procedures apply for listing individuals on the UN terror list. During the inspection, the Committee asked to be kept informed about this work. In the light of this, the Committee has familiarised itself with the rules relating to entries on the UN list.

The UN Committee of Sanctions consists of representatives from all 15 member states in the Security Council, which is responsible for imposing sanctions against the Taliban regime in Afghanistan as a consequence of the regime's support of Al-Qaida and Osama bin Laden. Entries on the sanction list require consensus from the member states that the person or organisation in question is a member of a group encompassed by the sanction regime. Any UN member state can propose that individuals, groups or organisations be listed on the sanction list and in that connection no charge or conviction is necessary.

Entries on the UN sanction list are not limited in time. Sanctions must be maintained for as long as the person or organisation is listed. All individuals, groups or organisations can apply to have their case reassessed. Formerly, this could only be done by applying to the national state or state of residence which would then decide if the case should be brought before the committee. Through a 2006 amendment, access was given to direct such a request directly to a UN contact point. The access to do so was established on the basis of raised criticism concerning the lack of procedural rights for private individuals, particularly in the form of an opportunity for contradiction and access to a review of the decision basis for the listing. Also decisions to delete names from the UN sanction list require consensus.

In December 2006, Najmuddin Faraj Ahmad (Mullah Krekar) was entered on the UN list. As far as the Committee is aware of, he is the only individual with residence in Norway whose name has been listed by the UN Committee of Sanctions. In 2008, the Committee will keep itself informed about the Norwegian authorities' implementation of list entries and any obligation the authorities might have to report supplementary details to the UN Committee of Sanctions.

IV. THE NATIONAL SECURITY AUTHORITY (NSM)

1. Inspections, general about the supervision of the Service

The inspection activities in the NSM follow a regular pattern. An account is provided about the ongoing activities in the Service since the last inspection. In addition, an account is usually given concerning one 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 goes through all negative complaints decisions at each inspection made since the previous inspection. Regular spot checks are also made on a number of negative security clearance decisions that have not been appealed, and which the NSM obtains in advance from the clearance authority requested by the Committee. The Committee also inspects the Services' electronic processing system for security clearance issues, as well as the NSM's records and archives.
In 2007, the Committee carried out four inspections of the NSM. Furthermore, inspections were carried out of the personnel security clearance service in three clearance authorities: the Armed Forces' Security Section (FSA), the County Governor of Vest-Agder and the Ministry of Foreign Affairs. In addition, the Committee inspected the intelligence and security functions in the Norwegian Home Guard.

The Committee received two complaints in 2007 which related to security clearance cases decided by the FSA and one complaint which was directed at the NSM. In 2006, the

Committee received two complaints relating to security clearances. Criticism was expressed in connection with one of the 2007 cases. This concerned the case processing in the FSA.

In many cases a security clearance is a prerequisite for obtaining or maintaining a professional position. Security clearance is particularly important for positions with the Armed Forces, as so many of the positions in the Armed Forces require security clearance. The regulations relating to security clearance stipulate a specific need for security clearance. This requirement can in some connections cause problems, cf. the case referred to in section 2 below.

By the amendment of the Security Act which entered into force on 1 January 2006, the conditions for granting security clearances to foreign nationals were relaxed. Section 22 of the Security Act now stipulates that: “a foreign national may be granted security clearance after an assessment has been made of the security-related significance of the person’s home state and his or her affiliation with their home state and Norway”. The affiliation with other states is also a relevant aspect in the assessment of whether security clearance should be granted to Norwegian citizens, cf. Section 21, first subsection, letter k of the Security Act. At the same time as the Act was amended in 2006, it was decided through an amendment of Section 3-3 of the regulations relating to personnel security clearances that the NSM must prepare so-called country assessments which the clearance authorities can use in granting security clearances to foreign nationals and Norwegian nationals with affiliation to other states.

In 2007, the Committee received an account of NSM’s work on country assessments. The main objective of the assessments is to provide the clearance authorities with relevant information which can be used in their preparation and implementation of security interviews and to contribute to the individual risk assessments in individual cases. The assessments contain information about the political system, religion, external relations, internal matters, defence, intelligence, the security-related significance of the country, the form of government, relations with Norway and other countries, crime picture and economic situation, etc. The assessments, which must be kept updated, are distributed to all clearance authorities. The assessments must be of a neutral character and are only meant as supplementary information to the case processing in individual cases. It should not be possible for the clearance authorities to refuse a person security clearance exclusively on the basis of the country assessment.

An important objective of the country assessments is to help make the assessments more correct. The Committee believes that it is also very valuable that the assessments promote the same treatment by different clearance authorities, as they would provide the clearance authorities with a common assessment foundation in a field where it cannot be expected that the individual clearance authority itself should have sufficient competence or knowledge. Furthermore, social developments increase the number of clearance cases where the main person or a closely related person is affiliated with another country.

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

In its 2006 annual report, the Committee referred to a complaint which concerned an authorisation as Restricted after the security clearance had been revoked. The Security Act stipulates that access to information classified as Confidential or higher requires security clearance (and subsequent authorisation), whereas only authorisation is needed for the lowest classification level Restricted. The authority to grant such authorisation usually lies with the employer, also in cases where the security clearance has been revoked. Persons whose security clearance has been revoked may not, however, be authorised as Restricted without prior dispensation from the clearance authority. In the complainant’s case, the FSA had denied dispensation, without further specification of the reason.

In connection with the processing of the complaint case the Committee asked the NSM to look into the reason for the dispensation refusal in more detail. Such a dispensation would be decisive for whether the complainant could continue his employment with the Armed Forces. After reviewing the case again the NSM granted a dispensation in May 2006 so that an authorisation could be considered in the case. Despite NSM's dispensation, the issue of the complainant's authorisation was not assessed by the employer. The reason for this was that the position that the complainant had held had been discontinued due to a reorganisation of the Armed Forces. Consequently, there was no current need for authorisation.

When the observation period for the complainant's decision for security clearance refusal expired in July 2006, the Armed Forces' Personnel Service (FPT), which the complainant had then been transferred to, submitted a security clearance request for Secret to the FSA. The request was returned by the FSA who questioned the need for the security clearance. The FPT then submitted a new request for Confidential. The reason for the request was that the person concerned was in the category "Personnel without a position". The FPT did not have a specific position to offer the complainant, but wanted to ascertain whether he could be given a security clearance. They had experienced that without a security clearance it was practically impossible to relocate personnel without a position and that the alternative in such cases is to make such personnel redundant. The request for security clearance at the Confidential level was reviewed by the FSA. At the same time, the FSA stated that they would look into the general question of the power to grant security clearances to such personnel in more detail.

In the 2006 annual report, the Committee gave an account of the issue and stated that it would keep informed about the further processing in the FSA, both regarding the general issue and the case of the complainant. In their review of the annual report, the Standing Committee on Scrutiny and Constitutional Affairs stated that they found it unsatisfactory that the case had not yet been resolved and asked to receive information about the further processing of the case and about the general questions relating to the security clearance practice in connection with the Committee's annual report for 2007.

The Committee has followed up the case in 2007. In reply to the Committee's written question, the FSA stated that the complainant's security clearance status was still Confidential, but that a new security clearance request for Secret had been submitted by the FPT. The reason for this was that it was not possible to find a position for the complainant with a security clearance of Confidential, as all the relevant positions required a Secret security clearance.

As concerns the general question relating to the security clearance practice the FSA stated that:

> "No work is currently ongoing in the FSA regarding "the general question of the power to provide security clearance for personnel in the Armed Forces who are without a position". In the FSA's opinion, we are not authorised to initiate inspections of individuals or to grant security clearances for personnel without a justified need for security clearance in connection with a position or other assignment/other service for the Armed Forces where one might have access to sensitive information. We refer to Section 19 of the Security Act, cf. Section 3-1, first subsection of the regulations relation to personnel security clearance. In the FSA's view, personnel in the Armed Forces must, as a minimum, be proposed for a position where the relevant security clearance level is stated before a request for security clearance can be considered.
>
> The FSA has previously processed security clearance requests without a real and specified need. Reference can in this connection be made to the fact that the FPT has expressed a need and desire to security-clear personnel without a position as they are instructed by the

Defence Staff (FST) to administer this group. The request for security clearance at Confidential level for [the complainant] was being processed for reasons of “principle”, without this being specified in more detail…The FSA regrets that we previously have given ambiguous signals and followed a somewhat unclear practise concerning the issue of security clearances for personnel without a position/a specified need.”

In its conclusive letter to the FSA, the Committee commented as follows:

”Pursuant to the FPT’s account there is no reason for the Committee to presume that [the complainant] relating to the transfer of Personnel without a position were handled any differently from other types of personnel whose security clearance is revoked. The issue which will remain unsolved in this case is how the [complainant’s] position in the Armed Forces would have developed if the FSA had granted dispensation rights in June 2004, as should have been done according to the regulations, or if the NSM had looked into the question of the handling of the [complainant’s] complaint in the security clearance case of their own initiative.

The FSA’s handling of the FPT’s subsequent security clearance requests for [the complainant] has been characterised by the existing disagreement between the FSA and the FPT regarding what security clearance need personnel without a specific position in the Armed Forces’ Military Organisation (FMO) might have.

Pursuant to Section 19 of the Security Act any person who ”might gain” access to sensitive information shall undergo prior security clearance and receive authorisation as necessary. It follows from the preparatory works that the expression “might gain” has been chosen to include categories of personnel who through their work are in a position where such access can easily be obtained. This includes for instance cleaning personnel. Consequently, the provision does not specify that it must be documented that the person in question “will have” access to sensitive information. The discussion relates to specific positions. This means that the preparatory works cannot be considered to give conclusive guidance for the current issue. Nonetheless, it can be said that the wording of the Act – might gain – does not preclude a broader interpretation than that the need must be linked to one specific position. Moreover, the provision is interpreted in such a way that the need for security clearance is sufficiently justified when someone has been recommended for a position. This implies that more people than the employed person may receive security clearance.

It is correct as the FSA writes that a person without a real need for security clearance should not be given one. In that respect reference is made to Section 3-1 of the regulations relating to security clearance of personnel which instruct the clearance authority to reject security clearance requests that are not properly justified and documented. This requirement has been reinforced in recent years to avoid that the security clearance institution is misused for unauthorised checks of employees’ conduct. Generally, there are therefore grounds for precise requirements for the need for security clearance.

However, it is difficult to see that there is any significant risk of this type of misuse in connection with the submission of security clearance requests for the group of personnel discussed here. Personnel without a position are, as far as the Committee understands, FMO employees who are redundant as a result of re-organisations or for other reasons and who, pursuant to the acts and regulations, should be prioritised for positions that they are qualified for within the organisation. Presuming that it is correct what the FPT writes, i.e. that most positions in the FMO are of the security clearance level Secret, it does not seem immediately unreasonable or at variance with the wording in Section 19 of the Security Act to say that this personnel have a sufficiently close and specific need for security clearance for them to request security clearance whilst being relocated. The main objective of the provision in Section 19 of the Security Act is to protect the individual against misuse of the institution. However, in the cases described in the above, the lack of security clearance is a disadvantage for the individual and could result in them losing their job.

It is possible that there is another side to this issue. This relates to how applicants without security clearance are treated in competition with applicants with security clearances. It may be that applicants with valid security clearances enjoy a simpler and speedier application process and that they in fact are preferred for that very reason. If that were the case, it would be unfortunate. However, there is no reason to investigate this issue further at present as the Committee is of the opinion that the security clearance rules allow for such a disadvantage to be remedied, given that the FPT's information about security clearance levels is correct.

It should in any circumstances be a requirement that the Armed Forces' security clearance authority adopts an active attitude towards solving this problem, in one way or another. The FSA writes in their letter that no work relating to this issue is being carried out at present and the impression is that the FSA has taken their stand and that they see no reason for further action. The Committee would like to point out that as long as it is maintained that redundant personnel in the FMO are prevented from an efficient relocation process when they do not have a security clearance, the very least the FSA could do is to raise the issue with the superior expert authorities in the NSM and possibly also with the FPT. It is clearly unacceptable to have a situation where it is not possible for personnel to obtain a job because of the lack of security clearance and where it is not possible to obtain security clearance because they have no job.

In the light of this, we request that the FSA take the necessary initiatives for a speedy clarification of the general question relating to the need for security clearance for this group. Furthermore, the Committee assumes that the existing security clearance request for [the complainant] is processed without further delay. It is now almost two years since the [complainant's] observation period expired, but he has still not been given a new position. As regards the specific assessment of his case, the Committee would like to point out that it is not immediately obvious why there are grounds to grant a security clearance for Confidential, but not for Secret, if the assessment is related to the need for security clearance."

The Committee will follow up the further handling of both the general question concerning security clearance right for personnel who are being relocated and of the complainant's case.

3. Two cases of breach of document security in the Armed Forces

In the 2006 annual report, the Committee drew attention to two cases of breach of document security in the Armed Forces. The cases were presented to the Committee as being so extensive that they pointed to a deficiency in the Armed Forces' document security system. The fact that it took such a long time before the internal responsibilities were dealt with, combined with the fact that the Committee has on previous occasions observed that individuals in the Armed Forces who have committed breaches of document security have been dealt with severely in individual cases, also raised questions about the principle of equal treatment.

The first case concerned a former officer who had kept several thousand pages of classified documents at his private residence. When the case was investigated it was discovered that it was mainly a case of Restricted documents. Approximately 100 documents were of a higher classification. In accordance with the regulations relating to security administration, the FSA has carried out a damage assessment of the documents classified as Confidential or higher. The case has been the subject of thorough scrutiny and the Armed Forces' routines for document security and security-related administration have been assessed in the process, as has the issue of personnel responsibility. However, according to the Committee's information, no damage assessment had been carried out of the documents that were classified as Restricted, as the regulations to the Security Act do not stipulate such a requirement for documents of the lowest classification level. Nor had any other analyses been performed with regard to these documents.

The scope alone made the Committee take up the issue. According to the Committee's experience, a breach of document security even at the lowest level might have serious consequences in individual cases with regard to security clearance. This did not correspond well with the lack of concern for potential shortcomings in the document handling routines or internal control routines, when such large quantities of documents had been removed from the archives or copied. The issue was raised with the NSM who stated on a general basis that large-scale compromising of several documents classified as Restricted could in total have greater potential for damage then compromising one document with a higher classification, and that this might be of significance to the response to the breach of the document security rules. With regard to the case in question, the NSM stated the following:

> "In this connection, it should be pointed out that in our letter of 6 July 2007, the NSM proposed to the Chief of Defence a thorough examination and follow-up of [the case] which will ensure that the necessary mitigating measures are in place with regard to the information in the compromised documents and which will, furthermore, ensure that Norway can fulfil its obligations in accordance with the NATO regulations in a satisfactory manner. The follow-up of the case, including the procedures for response to security-threatening incidents, has been reviewed together with the FSA. In the event of the compromising of large quantities of documents classified as Restricted, a damage assessment should, in the NSM's opinion, also be conducted of the total amount of information ... The NSM appealed in the above-mentioned letter to the Chief of Defence that such an assessment should be carried out. This is not clearly expressed in the requirement for damage assessment, cf. Section 5-2 of the regulations relating to security administration. However, the NSM maintains that the objective of the regulations' provisions on damage assessment calls for this to be carried out when the scope of the compromised documents classified as RESTRICTED is extensive, which must be said to be the case [in the case]."

In the light of the NSM's reply, the Committee did not find grounds for following up this issue any further. However, the Committee will keep itself informed about the initiative the Service has taken towards the Chief of Defence.

The other case which was mentioned concerned extensive rests of classified documents which emerged in connection with Headquarters Defence Command Norway's move from Camp Huseby. This case bore evidence of the Armed Forces having had insufficient routines for document security. The FSA has provided the Committee with an account of this case. Upon examination it emerged that in most cases it was a matter of insufficient office routines, as most of the documents had either been returned to the archives or been shredded, but without this having been recorded in accordance with the regulations. The FSA has informed the Committee that several measures have been implemented to improve the document security in the Armed Forces. Furthermore, the FSA has initiated general efforts to increase awareness of preventative security work. Investigations are ongoing in cases where there is a lack of overview of registered copies. This case will also continue to be followed up by the NSM.

4. Shredding stop for the clearance authorities

In 2003 a temporary shredding stop was introduced for the clearance authorities. The reason for this was that people who had gained access to PST's archives might also need access to the archives which had received information from the PST. The shredding stop came into force for cases from the period 8 May 1945 to 8 May 1996. Spot checks of NSM's case handling system showed that the NSM and the clearance authorities practised a total shredding stop for all security clearance cases, also for documents of a more recent date than 8 May 1996.

The Committee raised the issue with the NSM who notified us that the service would start to shred cases of a more recent date than 8 May 1996. This work was to follow the general rules stipulated in the regulations relating to personnel security clearance concerning storage

and discarding of information. The rules stipulate that the clearance authorities must discard information in security clearance cases after the preservation period has expired. This entails that the information must be reviewed for discarding when the person concerned no longer holds a valid security clearance. As a security clearance case must be kept for five years security clearance cases had accumulated for the period 8. May 1996 to 2002 that were now ready to be assessed for discarding. A significant backlog had thus accumulated.

When the Committee raised the issue with the NSM again a year later, the service informed that the discarding work had been delayed due to a lack of resources. The Committee replied to this in a letter to the NSM stating:

> ”The reason for the shredding stop was that persons who had gained access to the PST’s archives may also need access to the archives that have received information from the PST. The material is also of historical value. These considerations do not apply to more recent security clearance cases and out of consideration for the individual it is of great importance that the rules relating to discarding are followed in practice. Moreover, the information in a security clearance case is of a relatively sensitive character and storage beyond the necessary period should for that reason be avoided.---”

The NSM stated in their reply to the Committee that a plan for discarding had now been prepared which will be used for a systematic reduction of the remaining documentation. This meant that no further follow-up was necessary. The shredding stop for the PST was abolished on 1 January 2008, cf. Paragraph 2.2 in the chapter on the Norwegian Police Security Service. The clearance authorities will now also start discarding cases for the period 8 May 1945 to 8 May 1996. The Committee will pay close attention to this work.

5. Inspection of the procedures for security clearance cases in the Public Construction and Property Management Office (Statsbygg)

During its inspection of the NSM in August 2007, the Committee asked to be presented with non-appealed negative security clearance decisions made by Statsbygg. On the basis of the facts that emerged during the Committee’s review of the cases, the Committee raised some issues of a general nature in its letter to Statsbygg concerning their handling of security clearance cases relating to the reasons given the person in question, concurrent internal reasons, case information and stipulation of the observation period. In all these areas the Committee’s random checks gave the impression that Statsbygg’s case handling procedures were not congruent with the requirements stipulated in the Security Act and the regulations relating to personnel security clearance. The Committee had no comments concerning the decision on the merits of some of the reviewed cases.

In their reply Statsbygg acknowledged that the case handling routines for all of the areas reviewed by the Committee had not been in conformity with the regulatory requirements. During the summer and autumn of 2007, Statsbygg was allocated more resources and increased expertise to handle security clearance cases, and the routines have now been reorganised. Statsbygg gave a thorough account of this. After this the Committee only had the following remarks:

> ”The obligation to provide grounds for decisions concerning security clearance is important for many reasons. It is to ensure notoriety and render checks possible through access requests, for appeals and external controls. However, it is perhaps most important for the individual assessment of the cases. This was in fact one of the reasons for the introduction of the rules relating to the obligation to provide grounds in security clearance cases – as it enforces an unbiased balancing between the different considerations in each case. Both the external and internal grounds contribute to this. But it is particularly the internal grounds containing all the information in a case that are significant. There are reasons to point out that the practice has not been in conformity with the regulatory requirements on this point. In the two individual cases where the persons in question were not notified of the decision and their right of appeal, we request that such notification and a statement of the grounds for the decision are sent out now, with an explanation for the delay. The persons concerned should then be given the rights they are entitled to. For information purposes, the Committee would appreciate a copy of the notification. Should

Statsbygg have any objections to providing the persons in question with a notification and statement of grounds, we would like to receive an explanation for this.

The purpose of stipulating an observation period is to provide the individual with predictability for when a security clearance at the earliest can be granted – following a new check and assessment of the person concerned. The observation period is also useful for the employer (the person responsible for the authorisation) with a view to available personnel and planning of when a new security clearance request may be submitted if necessary. As we understand, Statsbygg handles a relatively large number of security clearance cases for employees in private companies. We presume that it is of special significance for this category of personnel that it is specified when a new security clearance request can be submitted. The length of the observation period says something about the gravity of the reasons for the negative decision and may be useful also on this basis, if a reason for the stipulation has been specified. In the light of this, there is reason to point out that Statsbygg has failed to comply with the statutory rules also on this point."

6. Inspection of the procedures for security clearance cases in the Ministry of Justice and the Police

For the inspection of the NSM in August 2007, the Committee also asked to be presented with non-appealed negative security clearance decisions made by the Ministry of Justice and the Police. On the basis of their review, the Committee questioned the Ministry on several points relating to their procedures and a more detailed reason was requested concerning two decisions on the merits.

It was apparent from the Ministry's reply that they had not had established routines for the preparation of internal, concurrent grounds, as stipulated in Section 25, last subsection of the Security Act. The usual practice had been that the executive officers would discuss the issues verbally and take notes in the form of keywords. These would not be filed under the cases. The Ministry informed the Committee that this practice had changed as a result of our letter. The Ministry stood by the decisions on the merits and accounted for their reasons for this.

In its final letter to the Ministry, the Committee stated the following relating to the issue of the obligation to provide grounds:

> "The Ministry's former practice of verbal assessments and notes does not comply with the stipulation in Section 25, last subsection of the Security Act relating to the preparation of internal, concurrent grounds which must comprise "all relevant matters".
>
> The obligation to provide written grounds is perhaps most important for the individual assessment of a case. Part of the reason for the introduction of the obligation to provide grounds was that it will enforce an unbiased balancing of the different considerations in each case. It is therefore an important rule, which we hereby point out that the Ministry did not comply with until questioned by the Committee. In the light of the Ministry's regret and the information about the change in practice, the Committee sees no reason for further follow-up."

The Committee had the following comments concerning the two individual cases:

> "Security clearance case concerning […]
> In light of the pronouncements of judgements and the divergence between the printout from the register and the information on the personal data form, the Committee finds no reason to make conclusive objections to the Ministry's assessment of the decision on the merits of the case. However, it must be pointed out that in our experience the work performed by a police officer often carries a risk of complaints, sometimes for no good reason. Consequently, it is particularly important in these connections to be cautious of attaching any negative emphasis to the officer having been reported without further investigation. The severity of the matters that have been settled in this case is also difficult to assess exclusively on the basis of the information in the register. In the Committee's opinion, further investigations should have been conducted in this case, including procurement of police documents and by conducting a security interview.

In the NSM guidelines to Section 4-4, second subsection of the regulations relating to personnel security clearance, it is stated that when assessing the length of the observation period ”emphasis should be placed on the seriousness and nature of the matter, time elapsed since the perpetration occurred, the age of the person concerned at the time of perpetration, his/her life situation, etc.”. As no internal grounds have been prepared in this case by the Ministry of Justice and the Police, it is not possible to see what assessments have been used as basis for the stipulation of the observation period. Nevertheless, in view of the facts in the case, the Committee is of the opinion that the stipulated observation period is not in line with the practice of the NSM or other clearance authorities. Nor is the Committee aware of any other clearance authorities having established a general rule that an observation period of five years should be stipulated if there are “findings of several offences and at least one of these has not been settled”, which the Ministry refers to as their main rule. The fact that a criminal case has not been settled clearly does not justify a particularly long observation period, as one in such a case does not know the outcome of the case. The use of fixed rules in this area is unfortunate, not least because it can easily result in the cases not being assessed on an individual basis.

A negative clearance decision is incriminating. When it, as in this case, is maintained for five years, the risk of it being significant for the person in question increases. In the light of this, we request that the Ministry consider changing the fixed observation period in accordance with Section 4-1, fifth subsection of the regulations relating to personnel security. The Committee presumes that the NSM as an expert authority will be able to provide general guidance concerning the practice of this provision relating to the stipulation of the observation period.

Security clearance case concerning […]
The Committee was informed that the reason for the refusal was that a restraining order had been issued for […] to prevent him from seeing his former common-law spouse and that he ”was about to go abroad for a prolonged period”.

It emerges from the source results that a restraining order was issued for [...], but that the case, in which he was suspected of making threats (Section 227 of the General Civil Penal Code), was dropped because the application for prosecution was withdrawn. It seems somewhat unclear from the case documents what was the reason for the restraining order. In the Committee’s opinion, this indicates that the Ministry in the security clearance case should have obtained the police documents, cf. the requirements relating to case information stipulated in Section 21, third subsection of the Security Act.

Moreover, it is difficult to see that [...’s] three-week visit to Morocco in 2007 need be of any significance for this person’s security clearance. The same applies to his intention to marry a woman of Moroccan nationality.

The case bears evidence of having been settled on the basis of partly unsubstantiated and diffuse information. This is unfortunate, particularly because the case concerned security clearance needed for employment purposes, i.e. the decision would be decisive for the person concerned’s employment situation. In such cases it is necessary to set strict requirements for the case handling. In the Committee’s opinion this case should have been more thoroughly elucidated.

Also in this case an observation period of five years has been set, partly because of his intention to enter into marriage with a Moroccan woman. When stipulating the length of the observation period, great significance can hardly be attached to such a prospective relationship. In this light the Committee requests that the Ministry also in this case considers amending the fixed observation period in accordance with Section 4-1, fifth subsection of the regulations relating to personnel security.

The Committee awaits a response to the points where the Ministry has been requested to further assess the cases.”

7. Inspection of the personnel security clearance service in the Ministry of Foreign Affairs

In October 2007, the Committee conducted an inspection of the personnel security service in the Ministry of Foreign Affairs. After the inspection, the Committee wrote to the Ministry questioning the Ministry's authorisation regime for their own employees, their practice concerning the lack of personal history data for closely related persons affiliated with other states and the handling of the Ministry's so-called "ad doss" files (*secret personnel files*), etc.

The Ministry gave a thorough account of the issues raised. As regards the ad doss files, the Ministry stated that these had previously been reviewed and thereafter closed and that any documents relating to security clearance of current employees had been transferred to the personnel security archives.

In its final letter to the Ministry, the Committee urged the Ministry to go through the ad doss file cases relating to personnel who had left the Ministry and assess whether these should be shredded in accordance with Sections 6-8 and 6-9 of the regulations relating to personnel security clearance.

As regards the authorisation regime and the Ministry's practice in cases concerning close relations with foreign affiliation, the Committee stated the following:

> "Routines for authorisation of employees
> In the Committee's view, the continued lack of compliance with the regulations for authorisation of employees in the Ministry of Foreign Affairs is worthy of criticism, in the light of the safety-related considerations upon which the authorisation regime is based and the amount of time that has passed since the issue was first brought to the Ministry's attention by the NSM. As the Ministry has confirmed that it is working actively to implement an approved authorisation regime, the Committee has no further comments, assuming that the Ministry meets the deadline stipulated by the NSM concerning compliance with the regulatory requirements for authorisation.
>
> Closely-related persons' affiliation with other states
> Pursuant to Section 3-7, first subsection of the regulations relating to personnel security clearance, it is a requirement that relevant security-related information is available for the last ten years for persons encompassed by the control of individuals. For security clearances on a Secret level this also means the spouse, cohabitant or partner as well as the person concerned. For stays in a foreign state, Norway must have a security-related cooperation with the country in question for the obtained information to be used, cf. also Section 3-5.
>
> Pursuant to Section 3-7, second subsection, a security clearance may still be granted even if the 10-year requirement has not been fulfilled on the basis of an "individual total assessment". The provision states that in the assessment, emphasis must be placed on how many years of personal history is missing, whether the person concerned has served the Norwegian state and whether the lack of history is caused by conditions that are of little significance for national security. The provision herein is not meant to be exhaustive.
>
> The Ministry states that if the closely related person's lack of personal history is associated with his/her work or assignments for the Norwegian authorities, humanitarian organisation, etc, the issue will not be pursued further. Moreover, the Ministry states that closely related persons who are living abroad because of their spouse's work for Norwegian authorities, etc. are also comprised by this practice.
>
> The Committee cannot see that what the Ministry expresses herein is in keeping with the requirements laid down in Section 3-7 of the regulations relating to personnel security clearance, nor with what is stated in the NSM's guidelines to the provision. The guidelines read that closely related persons' work for governments and organisations as mentioned should normally not be of significance for the main person's security clearance. The situation

where the close relation's expatriation is the result of their spouse's/partner's work for Norwegian authorities, etc. is not dealt with in the guidelines.

The Committee realises that practical issues may arise in connection with expatriation if the requirement relating to personal history for closely related persons were to be strictly enforced. However, it is a fundamental requirement of the regulations that an individual assessment must be conducted on a case-by-case basis, i.e. one must examine if there are any circumstances relating to the lack of personal history which could warrant further investigations. In particular, an assessment must be made of the duration of the stay, the country's intelligence-related threat to Norway and the country's security-related significance, as well as the reason for the stay abroad. If there is any doubt as to the person in question's understanding of security in relation to the spouse's/cohabitant's/partner's expatriation in a state which Norway does not have a security collaboration with, the Act stipulates that a security interview must usually be conducted. This must be conducted in all cases where "it is not obviously unnecessary", cf. Section 21, third subsection of the Security Act.

In the Committee's opinion, closely-related persons accompanying their spouse/cohabitant/partner on an expatriate assignment for Norwegian authorities, etc. should not receive any special treatment. A case-by-case overall evaluation must be conducted also in these cases before a security clearance can be granted. If, for instance, an employee in the Ministry of Foreign Affairs marries a person from a country that Norway does not have a security-related collaboration with and which may pose an intelligence-related threat to Norway, the significance this has for the person in question's security clearance must be subject to evaluation. This applies regardless of whether the person in question works for the Norwegian state in Norway or abroad.

According to this, the Ministry of Foreign Affairs' practice of emphasis on matters to do with closely related persons in cases concerning security clearance does not seem to be congruent with the security legislation's requirements. The Committee requests that the Ministry conduct a more thorough evaluation of the issues expressed herein, with a view to a potential readjustment of the practice. To the Committee, the principle of equal treatment is a major point in this case. It is problematic if a major clearance authority establishes a practice which is more liberal than the practice followed elsewhere, on the basis of guidelines from central expert authorities, cf. in this connection the last complaint case commented on in the following. It must also be pointed out that, considering how practical this problem must be for the Ministry's cases, it would have been natural if the Ministry discussed with the NSM, in their capacity as expert authority, how this practice should be organised."

The Committee will continue to follow the Ministry's further actions on these issues.

8. Inspection of the intelligence and security functions in the Norwegian National Guard

In January 2007, the Committee carried out an inspection of the intelligence and security functions in the Norwegian National Guard. The inspection was carried out among the National Guard Staff. The Committee was informed about the duties and organisation of the National Guard and about the activities of the Guard committees' activities and was then given a more detailed account of the intelligence and security function of the National Guard, and about the preventative security work. An inspection was carried out of the records relating to the security and intelligence functions, including their functions as authorisation authority and requesting authority. The inspection did not give any grounds for follow-up by the Committee.

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

9.1 Introduction

The FSA processed approximately 23,000 security clearance cases in 2007. This amounts to two thirds of all security clearance cases resolved each year, and makes the FSA the largest security clearance authority in the country. The Committee conducted three inspections of the FSA in 2007. This is considered necessary to ensure a satisfactory control.

In the main, the Committee's inspections of the FSA focused on their capacity as a security clearance authority. The Committee is presented with all negative security clearance decisions since the last inspection for their review. In addition, inspections are carried out of archives and registers in the personnel security clearance department. As the FSA processes a great number of security clearance requests each year, the workload is significant. In 2007, the FSA has focused on reducing the processing time for these cases.

The Committee's general impression is that the FSA is continually working on establishing case processing routines to ensure compliance with the stipulations in the Security Act, and that the case processing and the decisions made generally are of a high quality. However, it appears that the FSA makes less use of security interviews than other security clearance authorities. The Act stipulates that security interviews be held in all cases unless it "is obviously unnecessary". This rule is a reflection of the general principle that the administration must ensure that all aspects of a case have been elucidated to the extent possible before a decision is made. In many cases a security interview will serve as an important basis for the security clearance authorities' assessment of whether the person concerned should be given a security clearance. For efficiency reasons the FSA often seeks to clarify doubts by first obtaining supplementing information from other authorities, such as records of court rulings, or by contacting sources by telephone. Providing that one complies with the rules for the recording of information obtained verbally and other rules for case processing relating to the gathering of information, such practice is in full compliance with the regulatory requirements. However, the Committee will follow developments in this field, as in many cases a security interview cannot be replaced by other types of information procurement and the Act does stipulate that security interviews should be held in cases of doubt. Efforts to reduce the case processing time should not be at the expense of the individual's legal protection.

The FSA also has other tasks in addition to their function as clearance authority, such as security intelligence activities in the Armed Forces. These are also included in the Committee's oversight duties. On behalf of the Chief of Defence, the FSA has duties that relate to the counter-acting of security threats such as espionage, sabotage and acts of terrorism that are a potential threat to the activities of the Armed Forces and national security. This work is performed by an operative security department of the FSA. In 2007, the Committee kept itself informed about the activities in the department and carried out inspections of the department's archives and registers.

9.2 Right of access when a security clearance case is dropped

In 2007, the Committee processed a complaint of the FSA's handling of an access request in a security clearance case.

The complainant had requested access to the information in his case. The case had been closed because the need for clearance had lapsed. The request was denied as the FSA did not consider that closing the case warranted a right to access, pursuant to Section 25a of the Security Act. A subsequent complaint concerning the refusal for access was refused by the FSA for the same reason. The FSA did not forward the case to the NSM as appealing body. A new petition for access from the complainant was also rejected by the FSA on the same grounds.

The complainant requested that the FSA look into the refusal of access and the failure to submit the case to the NSM as appealing body. The complaint was presented to the FSA who maintained that no clearance decision had been made at the point when the request for access was submitted. Thus, the complainant obviously did not have right to access at that point in time, pursuant to Section 25a of the Security Act, which stipulates that the access

right applies once a decision for security clearance has been made. The FSA found that the closing of a security clearance request was clearly not a decision about security clearance. However, the FSA added that one realised in retrospect that, on grounds of principle, the decision to deny the access request should have been regarded as an individual decision pursuant to Section 2, third subsection of the Public Administration Act and the complaint should have been forwarded to the NSM.

In our letter to the FSA the Committee wrote that according to both the preparatory works of the Act and in real terms, the closing of the case should be regarded as a security clearance decision. The Committee pointed out that a case closure can encompass many different situations where access might be necessary. In the light of this, it could hardly be regarded as obvious that there was no right of appeal pursuant to the Security Act as indicated by the FSA. However, the Committee did not come to a decision on this matter, but presented it to the NSM on a general basis.

As regards the FSA's failure to forward the access denial complaint to the NSM, the Committee stated that there were grounds for criticism despite the subsequent acknowledgement that the case should have been forwarded, as the FSA maintained for such a long time that the complaint should not be submitted to the appeal body. The Committee referred to the fact that it follows quite clearly from the Security Act and its reference to the Public Administration Act that there is a duty to forward a complaint to the appeal body even if the decision at first instance is a refusal. Thus the complaint relating to the decision to deny access should have been submitted to the NSM regardless of whether it was considered a decision on the merits of the case or a refusal of the request. The Committee maintained that the case should have been raised with the NSM under any circumstances as the NSM is the superior expert authority and the issue of right to access in a closed case was a matter of principle importance which had not been settled previously in a published decision or statement from the NSM or the Ministry of Defence.

9.3 Case processing time in cases concerning security clearance

In the 2006 annual report, the Committee commented on the case processing time in the FSA in cases where the control of individuals reveals findings in the registers, such as in the criminal case register or in credit information registers. The Committee was informed that the case processing time in the above-mentioned category (cases involving findings) may be very long, perhaps up to several months. The Committee expressed its concern about this as the consequences for the individual may be great. It could, for instance, affect the individual's chance of completing the compulsory military service as planned. It might also affect the individual's education or career with the Armed Forces. The Standing Committee on Scrutiny and Constitutional Affairs agreed with the Committee's view that the processing time should be reduced and asked to be kept updated on developments.

During the Committee's 2007 inspections, the FSA provided information about the backlog situation and the processing time for the various case categories. The FSA has been given extra personnel resources to reduce the processing time in security clearance cases. In this connection, the FSA also initiated a project in the personnel security clearance department to reduce old backlog. The project took place as team work, a work method the FSA has had good experience with. It emerged that it was often complicated cases that the department took a long time to process, where the opportunity to discuss the case with other case processors was particularly effective. The FSA informed the Committee that many older security clearance cases were resolved during the project period and that the backlog situation has improved considerably.

The FSA has stated that despite the positive development, the processing time is still too long for many case categories, but that they are now working systematically to reduce this by

sorting out and prioritising more urgent cases, i.e. the cases are no longer handled in strict order. The Committee has not come across individual cases in 2007 where the processing time in the FSA has caused problems for personnel conducting the compulsory military service. The Committee will follow the development through our inspections of the FSA.

9.4 Inspection of the FSA's department at Jørstadmoen and information meeting with FK KKIS

FSA's information security department consists of the section for security approval and the section for security support including the centre for the protection of critical infrastructure. The latter section is located at Jørstadmoen. Parts of the section's responsibilities used to belong to the former Norwegian Army Signal Corps.

In 2007, the Committee carried out an inspection of the department at Jørstadmoen. This was an ordinary inspection of an external department. However, part of the reason for the inspection was that the Committee wanted information on what types of technical equipment for wire-tapping/monitoring the Armed Forces have at their disposal. Besides information about the types of equipment at the Armed Forces' disposal, it is of interest for oversight purposes to learn what the equipment is used for and about the internal control of the use of such equipment. The Committee's technical expert took part in the inspection.

During the inspection, the Committee was given a briefing about the information security department, the centre for the protection of critical infrastructure, the operative work in the section and the types of communication monitoring equipment in the Armed Forces, including who is in possession of this equipment and what it is used for, as well as what control measures there are for the use of it.

The operative activities conducted by the centre for the protection of critical infrastructure come in under CND (Computer Network Defence). The activities mainly involve defending the Armed Forces' information systems by monitoring computer traffic on the networks. This makes it possible to detect attacks on the Armed Forces' information systems and implement measures to prevent computer attacks by analysing these attacks. These activities relating to the Armed Forces' information systems resemble the national critical infrastructure work that the NSM performs through NorCERT (Norwegian Computer Emergency Response Team). NorCERT has a cross-sectorial responsibility for both the military and civil section. During the inspection, the Committee was informed that the FSA's department at Jørstadmoen cooperates with NorCERT in certain fields.

The inspection did not give grounds for any follow-up by the Committee.

In connection with the inspection of the FSA department at Jørstadmoen, the Committee was given an overview of *the Norwegian Defence Forces Knowledge Centre Command and Control Information Systems (FK KKIS)*, which is working to coordinate and develop the opportunities for communication and data exchange in the Armed Forces. One of the areas the Committee requested information about was the establishment of a CNO unit (Computer Network Operations) in the Armed Forces placed under FK KKIS. The offensive part of the CNO activities will involve intrusion into other people's communications and computer networks. Also at this meeting the Committee was assisted by its technical expert.

V. THE INTELLIGENCE SERVICE

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

In 2007, the Committee carried out three inspections of the Intelligence Service HQ. Inspections were carried out of the Service's stations in Fauske and Kirkenes. A meeting was

held between some of the Committee members and the Intelligence Service. The Committee received one complaint directed at the Intelligence Service in 2007. The case has been concluded without criticism. The Committee did not receive any complaints directed at the Intelligence Service in 2006.

Last year's annual report stated that the Committee had, in consultation with the Service, decided to increase the number of annual inspections to three to provide a certain continuity. The increase to three inspections has been positive in as far as it provides the Committee with better continuity, something which is particularly useful in the technical field.

As in previous years, the 2007 inspection of the Service focused on the Service's technical information procurement. Moreover, the Committee has established a control regime in the course of the year for information enquiries from the Intelligence Service and disclosure of information to other collaborating services abroad.

Furthermore, in 2007 the Committee focused on the collaboration between the Intelligence Service and the PST. To be able to supervise the activities of each service it is important to gain insight into the intra-service collaboration. The 2006 instructions on collaboration between the two services, discussed by the Committee in last year's report, encouraged increased collaboration and the Committee has seen a certain increase in this field. This increase brings to light former untried questions and issues concerning the legal basis for the collaboration, cf. the discussion in Section 4 and 5 below.

Throughout the report year the Committee has corresponded with the Intelligence Service on issues relating to the understanding of Section 4 of the Intelligence Service Act which stipulates that the Norwegian Intelligence Service "shall not on Norwegian territory monitor or in any other covert manner procure information concerning physical or legal persons." This has helped clarify the Service's general view and provides a better basis for the processing of individual cases.

2. Inspection of the Service's technical information procurement

The Intelligence Service is continually developing their capacity and methodology for technical information procurement. Also in 2007, the Committee has been kept informed about this work. In its inspections of the Intelligence Service the Committee continues to place the greatest emphasis on the Service's technical information procurement. The Committee's technical expert has assisted the Secretariat in their preparation of the technical aspects of the inspections of the Intelligence Service and has assisted the Committee with their inspections. The technical expert has also been employed to brief the Committee on technical capacities and how the Committee best can control the use of these.

The new case processing and analysis tool for the processing of information collected by the Intelligence Service through their technical procurement activities, accounted for in the 2006 annual report, has now been completed. However, the new tool is continually being updated and developed. The system facilitates internal control by the Service. During the development of the tool the Service has maintained a dialogue with the Committee concerning how the tool can be used to facilitate the Committee's inspection. The system has both improved and simplified the Committee's control of the Service's technical information procurement, including the foundation for procurement assignments, what information has been procured and how the information has been handled by the Service.

The most important provision for the Committee's inspection of the Intelligence Service's technical information procurement is the injunction laid down in Section 4 of the Intelligence Service Act against monitoring or in any other covert manner procuring information concerning Norwegian physical or legal persons on Norwegian territory. To comply with this

prohibition it is necessary for the Service's technical procurement activities to be arranged in a manner that ensures that Norwegian objects are picked up and identified as soon as their nationality has been established. The Committee's inspection regime pays particular attention to the examination of this point. For more details on this topic, cf. to the discussion in last year's report.

The inspections carried out in 2007 have not revealed any cases where the injunction against the procurement concerning Norwegian physical or legal persons has been violated. Nor has the Committee found any other censurable aspects in connection with our inspection of the technical procurement activities in the Intelligence Service. Furthermore, the Service has provided satisfactory answers to the Committee's questions at the inspection meetings concerning these activities.

The complexity of and continuous developments in the technical information procurement make it necessary to spend a lot of time and resources on maintaining a relevant and efficient control. We are talking about a large amount of data. The Committee will continue to carry out inspections of these activities in 2008 as well.

3. Exchange of information with foreign collaborating services

In last year's report the Committee gave an account of the Intelligence Service's exchange of information with foreign collaborating services and the assessments the Committee made concerning the establishment of control routines for this exchange of information. In their assessment of the annual report the Standing Committee on Scrutiny and Constitutional Affairs asked to be kept informed about the progress of the work.

During 2007 the Committee has established a control routine for the Service's communication systems. To start with the control will concentrate on one larger communication system within counter-terrorism. The control is organised in such a way that the Committee can access the communication system and conduct searches and carry out spot checks of the messages sent by the Service. The control routine has been established in dialogue with the Intelligence Service and the Service has also in this field facilitated for the Committee' inspections.

The Committee has emphasised to the Service that if a need arises to make an exception from the Committee's right of access for the purpose of protecting sources, the Committee will be provided with information about the type of information that has been retained and the reason for the exception. Furthermore, the Committee has notified the Service that it will continually assess whether the control form is appropriate and adequate, if there is reason to carry out regular control of the communication system and whether there is a need to conduct searches and carry out spot checks of other communications also. These are matters that the Committee would like to consider in dialogue with the Service and this has been pointed out to the Service.

So far the inspection activities in this field have not given any grounds for follow-up by the Committee.

4. Political approval of methods and operations

In the 2006 annual report, the Committee reported a test case which had been raised with the Ministry of Defence concerning the scope of the Intelligence Service Act as an independent statutory basis for the use of intrusive methods, and how the fact that a method that has been assessed and approved by the responsible political authority will affect its legality.

After the Committee drew attention to the issue the Ministry of Defence carried out a thorough assessment of the problem, cf. the discussion in the 2006 annual report. The Ministry stated that political approval is necessary for new methods and that a failure to obtain approval in accordance with the circumstances may be significant for the question of whether the use can be deemed legal. Moreover, the Ministry also stated that an assessment would be carried out of whether written guidelines should be prepared to ensure a more visible and retraceable process for political approval, which may also include a judicial analysis in accordance with the circumstances. It was expressed that political clearance of methods and operations should take place in writing whenever possible, so that the approval is retrievable in the Service and controllable by the EOS Committee.

In connection with the Committee's 2007 inspection of a joint operation between the PST and the Intelligence Service (the case is discussed in Section 6, Chapter 3 and in Section 5 below), the Intelligence Service stated that the operation had been politically cleared in the Ministry of Defence. The Service could not initially document a verified approval from the Ministry – the operation was only mentioned in an internal memo which stated that the operation had been approved at a meeting in the Ministry. The Service subsequently obtained verification from the Ministry consisting of a handwritten endorsement confirming the Intelligence Service's description of the process. In light of this, the Committee deemed it necessary to bring the issue up with the Ministry in writing. Questions were raised concerning both the general assessment of the need for routines and the approval of the specific operation. The Ministry replied that their experiences so far had not revealed a need to change the rules, but that the Ministry would continue to focus on ensuring that the internal routines are good enough. As regards the case in question, the Ministry replied that it was presumed that the political clearance was recorded by the Service and filed with the case so that it would be retrievable and subject to the EOS Committee's inspection.

The Committee wrote the following to the Ministry:

> ”As pointed out in connection with our previous case concerning the legal aspects of the Intelligence Service's activities, it is important for the Committee's inspection of the Service that there are clear rules and routines for how methods and operations gain political approval and for the documentation of such approval. In cases where a new method or intelligence operation raise important legal issues, the Committee has stated that it should be evident from the documentation if these have been brought up during the approval process.
>
> This issue is illustrated by the specific case described by the Intelligence Service [...]. It does not emerge from the Service's internal memo what issues concerning the operation the Ministry was informed of prior to the operation, nor what assessments the Ministry made in connection with the political clearance. It was only after the Committee brought the issue of the political approval up with the Service that a comment was added to the memo by the Ministry confirming that the description in the memo complied with the Ministry's understanding of the case.
>
> The Committee would like to point out that satisfactory routines do not yet appear to be in place for notoriety and documentation of the political approval process concerning the Service's methods and operations. Nor does the procedure in this case seem to correspond with the practice described in the Ministry's previous correspondence […].
>
> As far as the Committee is aware of, the joint operation in question was of a new nature and raised relatively difficult issues concerning legal basis. The Committee would also for this reason like to point out that no other documentation of the process was presented, except for the above-mentioned memo.

> The Committee is not concerned with intra-ministry approval procedures, but wishes to see that satisfactory routines are established between the Ministry and the Service, so that it subsequently, besides the approval itself, is possible to see the actual basis for the process and – in view of the circumstances - what legal issues were presented for discussion."

The Committee asked the Ministry for a response to the general question about the need to implement better routines to safeguard the above-mentioned issues. The Ministry replied to the Committee's comments as follows:

> "The joint operation in question was of an urgent nature. The time aspect did not allow for a preceding written account from the Intelligence Service. The various aspects of the case and the Ministry of Defence's approval were discussed verbally and given at the meeting with the Ministry.
>
> As mentioned in our letter to the EOS Committee […] the Ministry expected the Ministry approval in this case to be recorded by the Service and filed on the case so that it would be retrievable and available for inspection by the EOS Committee. This was done, but in retrospect we realise that we should also have formalised the approval in writing, so that the Committee could check by personal inspection that this was available, without having to examine the Service's own records to ensure that such approval had been given.
>
> Our internal routines have been amended on this point so that ministry approvals that are put before the Ministry in future cases (pursuant to Section 13 of the regulations relating to intelligence services) are always formalised in writing – either through an endorsement on a written account/recommendation from the Intelligence Service or in a separate letter from the Ministry to the Service, proving that such approval has been granted. There will also in the future be cases that must be processed verbally due to the time aspect, so that the formalisation of necessity has to take place retrospectively."

In the letter the Ministry also raised certain issues of a general nature, including access to the approval process. This aspect of the case has not yet been concluded.

5. The joint operation between the PST and the Intelligence Service

As described in Section 6, Chapter III, the Committee carried out inspections of a joint operation between the PST and the Intelligence Service in 2007. The inspections of the Intelligence Service concern issues relating to the legal basis for their part of the operation. The Committee's examination of the operation is still ongoing and will not be discussed in more detail here. As regards the Intelligence Service, it still appears that according to the inspections that have already been carried out, uncertainty can easily arise concerning the scope of the existing legal basis when the PST as a national security service enters into operative collaboration with the Intelligence Service as an international intelligence service.

In the Committee's view, the Intelligence Service may also benefit from a review of the current regulations to assess how appropriate and clear the regulations are for this type of collaboration. The Committee is aware that the Intelligence Services' situation is different from that of the PST when it comes to legal basis, and that special considerations apply for this service. However, it seem clear that the change in the threat picture and the current operative need warrant a review and evaluation of the regulations, cf. the following paragraph on the general collaboration between the PST and the Intelligence Service. The inspections that have been conducted illustrate the practical issues that can easily arise when trying to join such different legal bases and that the regulations for the Intelligence Service have been drawn up with the fact that Intelligence Service is an international intelligence service in mind.

As regards the Committee's general assessment of the inspection responsibility in a situation where the regulations are unclear, reference is made to the comments in Chapter III, paragraph 6.

6. In general about the inspection of the collaboration between the Intelligence Services and the PST

Access to the collaboration between the Intelligence Service and the PST is important to the Committee's understanding of the activities and thus its ability to oversee the services. At present, there are set routines for the exchange of information and for the collaboration between the PST and the Intelligence Service. As regards the exchange of information, notoriety is consistently good, something which is vital for inspection purposes.

Inspections are conducted by requesting information during inspections of the services and through spot checks of archives and registers in the usual manner and of other communication networks that have been established.

In principle, the division of responsibilities between the PST and the Intelligence Service is simply that the PST has been assigned responsibility for threats relating to national security and vital public interests within the country's borders, whereas the Intelligence Service has equivalent responsibilities relating to the external threat. However, the international terror threat, where non-governmental players are predominant, combined with the developments in communication, has resulted in national borders providing a less meaningful demarcation for the threatening parties than previously and for the communications intelligence as a method. Thus practical demarcation issues relating to the services' responsibilities may arise more frequently than before. An important aspect of the Committee's oversight of the collaboration between the services will be to ensure that the services do not assist each other in such a way that it might entail an evasion of the regulatory framework stipulated for the services.

The regulations relating to the collaboration between the Intelligence Service and the PST (stipulated by Royal Decree of 13 October 2006) have facilitated a closer collaboration and exchange of information between the services. Pursuant to Section 1 of the regulations, this is one of the explicit purposes of the regulations. The Intelligence Service usually follows a practice where information concerning Norwegian citizens or foreign citizens living in Norway is submitted to the PST, if this information is considered relevant for the PST. This might be excess information from their own information procurement or from collaborating services. Vice versa, the PST may submit information to the Intelligence Service about individuals who are residing abroad. This may also consist of excess information from their own procurement or from collaborating services.

In 2007, the Intelligence Service and the PST have informed the Committee about a joint analysis project within counterterrorism, where the Intelligence Service contributes with analyses relating to issues outside the borders of Norway, and the PST with information on national issues. The purpose is to make the preventative work in the field more efficient, in particular through an increased understanding of the threat to Norway and Norwegian interests. Intelligence information is shared in the project and the services assess the need for intelligence measures together. The objective is to establish an agreed threat picture that will enable the services to provide Norwegian authorities with better threat assessments. The project has been conducted in 2007 and will continue in 2008. The Committee keeps continuously updated on the project work, both by requesting status reports for the project and by carrying out spot checks of the documents generated within the project framework.

In its discussion of the new collaboration regulations in the 2006 annual report, the Committee pointed out that the Ministry of Defence and the Ministry of Justice and the Police

had, pursuant to Section 8, last subsection of the regulations, been given the opportunity to establish a joint unit between the services for inter alia the production of joint threat evaluations and other intelligence analyses relating to international terrorism.

The Committee has been informed that a joint analysis unit between the Intelligence Service and the PST will be operative from 2 January 2008. Separate, unclassified guidelines have been prepared for the unit, which will be assembled when and if necessary. Together and on the basis of the information that each service possesses, the services will provide a description of current threat situations. Pursuant to the established guidelines, recommendations on security measures are not amongst the analysis unit's duties. The responsibility for such recommendations will rest exclusively with the PST, even if founded on a joint threat description. Initially, it has been decided that the analysis unit will be a trial arrangement for two years. The guidelines presuppose that the work will be well-documented, taking into account both the EOS Committee's subsequent inspection and the evaluation of the unit's work.

The Committee's general impression is that the services are aware of the problems that may arise from their cooperation with regard to factors such as the boundaries for the services' responsibilities and authorisations and the need for notoriety in the operative collaboration. Section 2 of the Cooperation Regulations stipulates that cooperation between the services must take place within each service's respective legal basis. This entails that specific assessments must be made concerning the legality of the operative cooperation. The services have informed the Committee that this is being done in practice. However, that this is a difficult area is illustrated by the issues discussed in Section 5.

The Committee will continue to oversee the current collaboration and exchange of information between the services in 2008.

VI. IN GENERAL ABOUT THE OVERSIGHT ACTIVITIES

1. Extraordinary rendition

In last year's report the Committee gave an account of the investigations conducted in connection with the PST's and the Intelligence Service's potential knowledge about the use of Norwegian airports for extrajudicial transportation of prisoners under the auspices of the American authorities (a practice which has become known as extraordinary rendition). The reason for the investigations was that the American authorities confirmed this practice in 2006. Moreover, there were speculations in the media that also Norwegian airports had been used for such transportation. The Committee's investigations gave no grounds for assuming that the services might have been involved in, or had any knowledge of, such activities. It was, however, unclear what information the Norwegian aviation authorities receive when foreign aeroplanes use Norwegian airports.

According to the information obtained by the Committee from the Civil Aviation Authority and Avinor, the information that the Norwegian aviation authorities receive when foreign aeroplanes use Norwegian airspace and Norwegian airports, is very limited. The information provided in such a connection relates to flight safety and collection of taxes and includes the aeroplane's registration number. However, the aviation authorities do not, for instance, receive passenger lists or information about the type of flight, etc. The investigations carried out by the Committee have not given any reasons to believe that Norwegian aviation authorities obtain knowledge which renders it possible for them to identify flights of this nature.

2. The relationship between the EOS services and the private security industry

The last few years have seen a development towards growth of private security companies in Norway as elsewhere. These companies offer a number of security and intelligence services, such as wiretapping, surveillance, hostage negotiations and bodyguard services. In other countries competitive tendering of public services now also includes certain duties within the police force and increasingly also military duties. These trends seem to be the same in Norway.

Both the police and the Armed Forces, represented by the FSA, are aware of this development and have during the past year carefully examined the development in their areas of responsibility and have prepared analyses and reports on current problems relating to the private security sector and the borderline between this industry and the organised services.

This development may also raise a number of issues relating to the oversight of the EOS services, as the duty of the Committee is to oversee ”the intelligence, surveillance and security services performed, managed or assigned by the public authorities”. The Committee has obtained and reviewed the above-mentioned reports that have been prepared and will follow developments closely in the time ahead.

3. Project work as a method

The way the Committee works is to a large extent determined by the stipulations in the EOS Instructions relating to the frequency and venue of inspections. Most of the Committee’s and the Secretariat’s time is spent on preparatory work and implementation of inspections, as well as on processing of internal cases in the Committee.

The current work does not allow for more methodical reviews of individual cases or individual areas. There might be a need for such reviews in several areas, as it would provide the Committee with a more sound foundation for its assessments. Such reviews may include individual cases of the services or the use of methods in these, topics they are working on or, for instance, the services’ practise of the regulations in certain areas. A possible project topic in the PST would be the Service’s use of coercive measures. As regards the NSM it might be necessary to look more closely into how the provisions in the Security Act are put into practice, including the regulations relating to security classification of information. A relevant area for the Intelligence Service would be the collaboration and exchange of information with the PST.

The introduction of project-based work is to a large extent a question of resources, as this work must come in addition to the ongoing work with inspections and meetings. The Committee will initially try out this work method to a limited extent and in consultation with the services to minimise their use of resources in such a connection. In light of the experience gained through the use of this type of work method, compared with the resources that are required, the Committee will consider if this is a way of working that should be employed as a permanent part of the oversight activities.

The Committee will provide an account of the experience gained in next year’s annual report.

4. International work and public disclosure

In previous annual reports the Committee has described the increase in international cooperation between the security and intelligence services in the work against international terrorism.

This development constitutes a great challenge for oversight committees in most countries. The international intelligence cooperation is regarded by the services as particularly sensitive and the oversight committees must respect that information from foreign services is barred from disclosure to a greater extent. Despite such limitations, the oversight committees have much to learn from each other. As always in international cooperation, it is most beneficial to cooperate with oversight committees from countries with similar systems, such as Canada, the Netherlands, Belgium, Sweden and the UK.

The organisation Geneva Centre for the Democratic Control of Armed Forces (DCAF) is also a good cooperation partner. The Committee will continue its cooperation with DCAF in 2008, and an international conference in Oslo is on the drawing board for the autumn of 2008. Moreover, the project-based work mentioned in the above will be developed through an exchange of experience with oversight bodies in other countries.

It is in the nature of the EOS Committee's work that it is not very accessible to the public, partly because much of the information is classified. However, there are still many aspects of the activities that can be discussed in the public sphere and that are being discussed in international forums. The Committee would here like to draw attention to the fine balance between security-political aspects and the individual's legal protection in a democracy. It is of great importance for the international cooperation that the annual reports are available in English and the Committee will from now on have their annual reports translated. Another objective is to publish the annual reports on the Committee's website in a more accessible format than previously. Furthermore, the Committee is considering following Sweden's example of translating the information about the Committee and possibly also the regulations into relevant minority languages.

VI. ADMINISTRATIVE MATTERS

1. Budget and accounts, etc

The Committee's expenses for 2007, including a transfer, amounted to NOK 6 070 696 compared with the budget of NOK 6 193 000.

In mid-December, the Committee moved into new offices in Akersgata 8, entrance from Tollbugata. The reason for the move was a lack of space and reduced security at the former offices in Nedre Vollgate 5-7.

2. Staff

The Committee's secretariat consists of Head of the Secretariat Hakon Huus-Hansen, Legal Adviser Henrik Magnusson, Legal Adviser Ingeborg Skonnord and Senior Executive Officer Lise Enberget, responsible for administrative tasks. The Committee Chair works part-time for the Committee.

Oslo, 12 March 2008

Helga Hernes

Svein Grønnern	Kjersti Graver	Trygve Harvold
Knut Hanselmann	Gunhild Øyangen	Theo Koritzinsky

Hakon Huus-Hansen

APPENDICES

1. **Information about the EOS Committee**
2. **The Act of 3 February 1995, No. 7 relating to the Monitoring of Intelligence, Surveillance and Security Services (the EOS Act)**
3. **Instructions of 30 May 1995, No. 4230 for Monitoring of Intelligence, Surveillance and Security Services (the EOS Instructions)**

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

Regional Secretary of the Norwegian Association of the Blind and Partially Sighted. 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

The Act relating to the Monitoring of Intelligence, Surveillance and Security Services

Act No. 7 of 3 February 1995

Section 1. The monitory body and the area to be monitored

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

Such monitoring 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 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.

Section 2. Purpose

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,

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 monitory. The Committee may not instruct the monitored bodies or be used by these for consultations.

Section 3. The responsibilities of the monitory committee

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

The Committee shall investigate all complaints from persons and organizations. 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 subjected to public criticism. Factors shall here be understood to include regulations, directives and 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 the first paragraph of section 1, 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 the second paragraph of section 43 of the Courts of Justice Act. Section 22-1 and 22-3 of of the Dispute Act shall not apply. Court hearings shall be held in camera and the proceedings shall be kept secret until otherwise decided by the Committee or by the Ministry concerned, 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. (the section has been repealed by Act No. 82 of 3 December 1999)

Section 8. Statements and reports

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 makes annual reports to the Storting about its activities. Such reports may also be made 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.

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.

Section 10. Assistance, etc.

The Committee may engage assistance.

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

Section 11. Penalties

Wilfully or grossly negligent infringements of section 4, the first and third paragraphs of section 5, the first and second paragraphs of section 9 and the second paragraph of section 10 of this Act shall render a person liable to fines or imprisonment for a term not exceeding 1 year, unless stricter penal provisions apply.

Section 12. Entry into force

This Act shall enter into force immediately.

Appendix 3

Instructions for Monitoring of Intelligence, Surveillance and Security Services (EOS)

Issued pursuant to section 1 of Act No. 7 of 3 February 1995 relating to the Monitoring of Intelligence, Surveillance and Security Services

Section 1. The monitory committee

The Committee shall have seven members including the chairman and vice-chairman, all elected by the Storting, on the recommendation of Presidium of the Storting, for a period of a maximum of five years. Steps should be taken to avoid replacing more than four members at the same time.

Those elected shall be cleared for the highest level of national security classification and according to treaties to which Norway is a signatory. After the election, authorisation shall be given in accordance with the clearance.

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.

Section 2. Quorum and working procedures

The Committee has a quorum when 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 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. 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.

Section 3. Conduct regulations

The secretariat keeps the case records and minutes. Decisions and dissents shall be recorded in the minutes.

Statements and comments uttered or recorded during the monitory process shall not be regarded as final unless they are reported in writing.

Section 4. Limitations, etc. of the monitory process

Monitoring responsibilities shall not include activities involving persons who are not resident in Norway and organizations that have no address in this country, or activities involving foreign citizens whose residence in Norway is associated with service for a foreign state. The Committee may however practise monitoring in cases such as those mentioned in this paragraph when special grounds so indicate.

The monitoring should be arranged in such a way as to interfere as little as possible with the day-to-day activities of the services. The Ministry prescribed by the King may wholly or partly suspend the monitoring during a crisis or in wartime until the Storting decides otherwise. The Storting shall be notified immediately of any such suspension.

Section 5. Limitations of access to information

The Committee shall not apply for more extensive access to classified information than is necessary for purposes of monitoring. It shall as far as possible observe consideration for protection of sources and of information received from abroad.

Information received shall not be communicated to persons other than authorised personnel or other public bodies who have no knowledge of it except when necessary in the course of duty, for monitoring purposes or as a consequence of the procedural regulations laid down in section 9. In cases of doubt, inquiries should be made of the person who supplied the information.

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 Chief of Defence and the Chief of the Norwegian Security Service Police.

Such protests shall be published in or be enclosed in the annual report of the Committee.

Section 7. Monitoring and statements

The Committee shall normally abide by the principle of subsequent monitoring, but may notwithstanding require access to information on current matters, and submit comments on such matters.

The monitoring and the formulation of statements by the Committee shall be founded on the principles laid down in the first paragraph and the first, third and fourth sentences of the second paragraph of section 10 and in section 11 of Act No. 8 of 22 June 1962 relating to the Storting's Ombudsman for Public Administration. The Committee may also propose improvements to administrative and organisational arrangements and routines when this may facilitate the monitoring or protect against injustice.

Before statements are made that may result in criticism or expressions of opinion being brought against the administration, the responsible superior officer shall be given an opportunity to make a statement concerning the issues raised in the matter.

Comments to the administration shall be addressed to the head of the service or body concerned or to the Chief of Defence or Ministry concerned when such comments apply to matters they should be familiar with as authorities responsible for issuing instructions and exercising control.

In the case of comments encouraging the implementation of measures or making of decisions, the recipient shall be requested to respond by giving notification of the actions that are taken.

Section 8. 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 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

Interviews with private persons shall take the form of an examination unless they are of a purely explanatory nature. Interviews with the administration's personnel shall take the form of an examination when the Committee finds it appropriate or when this is requested by civil servants. In matters that may result in criticism of specific officers, interviews should normally take the form of examinations.

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 instructions. The statement shall be read aloud before being approved and signed.

Persons who may be exposed to criticism from the Committee should be notified of this if they are not already familiar with the case. They have a right to familiarise themselves with the Committee's unclassified materials and with classified materials that they are authorised to examine, provided that this will not damage the investigations.

Any person making a statement shall be made aware of evidence and allegations that are inconsistent with the statement, provided that such evidence and allegations are unclassified or are on a level of security classification for which the person concerned is authorised.

Section 10. Investigations at the Ministries

The Committee may not demand access to the Ministries' internal documents.

If the Committee wishes to have access to information or statements from a Ministry or its employees concerning matters other than those applying to the Ministry's dealings concerning clearance and authorisation of persons and enterprises, these shall be obtained by written application to the Ministry concerned.

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 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 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 surveillance service: to monitor 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 all services: to ensure that the cooperation and exchange of information between the services is held within the framework of service needs.

2. Inspection activities shall at least involve:

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

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

c) six inspections per year of the Police Security Service HQ, involving a review of new cases and current 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 surveillance cases at least twice a year.

d) annual inspection of at least four duty stations in the external surveillance service, at least two duty stations in the local intelligence staff and/or intelligence/security service at military units and of the personnel security service of at least two Ministries/government agencies.

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

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

Section 12. Provision of 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 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.

The chairman or a deputy authorised by the Committee may otherwise provide information to the public concerning a matter that is under investigation as well as information as to whether the investigation has been completed or when it will be completed.

Section 13. Relations with the Storting

1. The provision laid down in the first paragraph of section 12 shall apply correspondingly to the Committee's reports and annual reports to the Storting.

2. If, in the view of the Committee, consideration for the Storting's control of the administration indicates that the Storting should familiarise itself with classified information in a case or a matter that the Committee has investigated, the Committee shall in a special

report or in its annual report to the Storting bring this to the attention of the Storting. The same applies if there is a need for further investigations of factors concerning which the Committee itself is unable to make any progress.

3. By 1 April each year, the Committee shall submit a report to the Storting concerning its activities during the previous year.

The annual report should include:

a) an outline of the Committee's composition, meetings and expenses

b) an account of inspection carried out and the results

c) a list of complaints sorted according to category and branch of service, specifying the results of the complaints

d) an account of cases and factors raised on the initiative of the Committee

e) a specification of any measures requested implemented and the results, cf. fifth paragraph of section 6

f) a list of any protests pursuant to section 5

g) presentation of matters or factors that should be dealt with by the Storting

h) the Committee's general experiences with the monitoring and regulations and potential need for changes

Section 14. Costs

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.

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

4. Specialists 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.