Abbreviated annual report for 2013

The Norwegian Parliamentary Intelligence Oversight Committee (the EOS Committee)

PREFACE

The Norwegian Parliamentary Intelligence Oversight (EOS) Committee is required to submit an annual report about its activities to the Storting. This abbreviated annual report for 2013 presents some of the main items from the more extensive annual report that is available on the Committee's website, www.eos-utvalget.no.

Chapter 1 describes the Committee's remit and composition. Chapter 2 describes important developments and challenges in 2013. Chapter 3 provides an overview of the Committee's activities in 2013: inspections, consideration of cases the Committee has raised on its own initiative, complaint cases and some important meetings, conferences and study visits in Norway and abroad. Chapters 4 to 8 provide information about the Committee's inspections of the different services and about cases involving matters of principles that the Committee has raised with the services.

The intelligence, surveillance and security services have generally demonstrated a good understanding of the Committee's oversight in 2013. Experience shows that the oversight helps to safeguard individuals' due process protection and to create trust that the services operate within their statutory framework.

1. THE COMMITTEE'S REMIT AND COMPOSITION

1.1 The Committee's remit

The EOS Committee is charged with continuously overseeing the 'secret services', i.e. the intelligence, surveillance and security services (EOS services) carried out by, under the control of or on behalf of public authorities. The EOS Committee's remit is set out in the Act relating to the Oversight of Intelligence, Surveillance and Security Services and in the Directive relating to Oversight of the Intelligence, Surveillance and Security Services. The acts, instructions and directives that regulate the services state that they are subject to oversight by the EOS Committee.

The Committee's primary function is to oversee that the EOS services do not subject individuals to unjust treatment. The Committee shall ensure that the services act within the framework of the law, regulations, instructions and directives, and respect human rights. Moreover, the Committee shall ensure that the activities of the EOS services do not involve undue damage to civic life.

The oversight is primarily carried out by means of inspections of the services' archives, computer systems and installations. Subsequent oversight is practised in relation to individual cases and operations. In principle, however, the Committee has full right of inspection and access and shall be kept continually informed about important ongoing cases. The Committee's oversight shall cause as little inconvenience as possible to the services' day-to-day activities. Particular account must be taken of the protection of sources and information received from cooperating foreign intelligence services.

The Committee investigates complaints from individuals and organisations. Any complaint or enquiry claiming that someone has been unjustly treated by the services shall be investigated in the service or services that the complaint concerns.

1.2 The composition of the Committee

The EOS Committee has seven members. They are elected by the Storting in plenary session on the recommendation of the Storting's Presidium for terms of up to five years. No deputy members are appointed. Members may be re-appointed.

The Committee is an independent body. Therefore, members of the Storting cannot also be members of the Committee. The Storting has emphasised diversity in the composition of the Committee, so that both political backgrounds and experience from other areas of society are represented. The committee members and secretariat employees must have top level security clearance, both nationally and pursuant to treaties to which Norway is a signatory.

The chair of the Committee is Eldbjørg Løwer, former government minister and deputy head of the Norwegian Liberal Party. The deputy chair is Svein Grønnern, Secretary General of SOS Children's Villages Norway and former Secretary General of the Norwegian Conservative Party. The other committee members in 2013 were Trygve Harvold, former Managing Director of the Norwegian Legal Database Foundation, *Lovdata*; Gunhild Øyangen, former Member of the Storting and government minister for the Norwegian Labour Party; Theo Koritzinsky, former Member of the Storting and head of the Socialist Left Party; Wenche Elizabeth Arntzen, District Court Judge in Oslo District Court and former advocate; and Hans Johan Røsjorde, former County Governor of Oslo and Akershus and Member of the Storting for the Progress Party. Røsjorde left the Committee on 25 October 2013, when he was appointed State Secretary at the Ministry of Justice and Public Security. Øyangen left the Committee on 31 December 2013.

On 10 December 2013 the Storting elected Øyvind Vaksdal, former deputy member and Member of the Storting for the Progress Party, and Håkon Haugli, former regularly attending deputy member of the Storting for the Norwegian Labour Party, as new members of the EOS Committee until 30 June 2016.

2 DEVELOPMENTS AND CHALLENGES IN 2013

In previous annual reports, the Committee has pointed to some national, international and technological developments that have a bearing on the work of the secret services and their oversight. Several of these developments have been evident in 2013 as well, for example in relation to the four challenges described below.

2.1 American authorities' surveillance abroad

Information that the American authorities have carried out surveillance abroad attracted international attention. Some of the surveillance has posed a challenge to trust and cooperation between countries, even between close allies. The documentation and subsequent debates have dealt with matters such as the intelligence services' legal authority, resources, methods and international cooperation; the role of the secret services in a democratic state based on the rule of law, and the potential conflict between protection of personal data and the need to protect the population and the state from terrorism etc.

2.2. International regulatory framework and cooperation between supervisory bodies

From a human rights perspective, there is a clear need for an international regulatory framework to protect the privacy of citizens against unlawful government and private surveillance. International cooperation between government supervisory bodies for the secret services is also necessary. *In recent years, the Committee has been in close contact with several foreign and international supervisory bodies, for example through seminars, conferences and joint publications, with a view to strengthening the exchange of information and advice to ensure more efficient democratic oversight.*

2.3 Greater transparency about the Norwegian Intelligence Service's international cooperation

International cooperation between secret services crosses boundaries, while oversight is limited to the national level. This makes transparency about intelligence activities and clear regulations governing the national services all the more important. It is positive that the supplementary provisions concerning the Norwegian Intelligence Service's (NIS) collection of information relating to Norwegian persons abroad and the disclosure of personal data to cooperating foreign services were made public in 2013. The EOS Committee routinely oversees the services' exchange of information with cooperating services. At the same time, the Committee complies with the Directive relating to Oversight of Intelligence, Surveillance and Security Services' instructions that 'Insofar as possible, the concern for protection of sources and safeguarding of information received from abroad shall be observed.'

In 2013, the Committee has followed up the issue of whether Norwegian citizens may have been subjected to unlawful surveillance in Norway as a result of international cooperation between intelligence and security services in relation to the Norwegian services. This is described in more detail in sections 4.7, 5.1 and 7.6.

2.4 Cooperation between NIS and PST

Cooperation between the different Norwegian services has also been strengthened in recent years, particularly between PST and NIS. This concerns counterterrorism, counterintelligence and work to prevent the spread of weapons of mass destruction, among other things. In 2013, NIS, the National Security Authority (NSM) and the Norwegian Police Security Service (PST) published a joint coordinated assessment of threats and vulnerability. The Committee was also informed about the establishment of a co-located counterterrorism centre, led by the head of PST and staffed by personnel from both services.

These cooperative measures provide more opportunities, but also present certain challenges: There are fundamental differences between the regulatory framework and tasks of PST, which is primarily to operate in Norway, and NIS, which can only carry out surveillance abroad. Each service is only permitted to obtain personal data and other data in accordance with the legal basis that applies to that service. *The Committee will continue to oversee that the services observe this principle in their cooperation.*

3 OVERVIEW OF THE COMMITTEE'S ACTIVITIES IN 2013

3.1 Inspections

More than a third of the Committee's inspections in 2013 have targeted PST, both PST Headquarters and local PST entities. The reason for this is the regulatory requirement for the number of inspections of that service. Pursuant to Section 11 subsection 2 of the Directive relating to Oversight of the Intelligence, Surveillance and Security Services, the Committee shall each year each year carry out at least:

- six inspections of the PST Headquarters (DSE)
- four inspections of the National Security Authority (NSM)
- three inspections of the Defence Security Agency (FSA)
- two inspections of the NIS headquarters

In addition, the Committee shall inspect:

- PST entities in at least four police districts
- at least two NIS and/or intelligence/security service functions in military staffs and units
- the personnel security service of at least two ministries or government agencies outside NSM.

The Committee conducted a total of 28 inspections in 2013, of which 16 at the central level. The Committee has inspected four local PST entities. The Committee has also inspected the personnel security service at PST Headquarters, the Norwegian Government Security and Service Organisation and the Ministry of Transport and Communications, as well as the intelligence and security service functions at Rena military base.

The Committee conducted three unannounced inspections in 2013. One of these inspections took place in connection with the investigation of the NIS's archive of sources, see section 7.2. The two other unannounced inspections was of NIS and the Intelligence Battalion, respectively, in connection with the follow-up of the investigation of the Intelligence Battalion, see section 8.4.

3.2 Complaint cases and cases raised on the Committee's own initiative

The Committee received as many as 47 complaints in 2013, compared with 21 and 29 complaints in 2011 and 2012, respectively. As a result of this increase, the Committee has used more resources than before on processing complaints. In addition, the Committee has received several enquiries by e-mail and telephone that have not formed grounds for opening complaint cases. Many complaints were against more than one of the EOS services. The Committee has rejected 16 complaints on formal grounds, particularly because the matter in questions did not fall within the Committee's oversight area or because the complaint was not sufficiently specific.

The Committee has raised 26 cases on its own initiative. The most important cases are described in more detail below in connection with the services they concern.

3.3 Meetings, seminars, lectures etc.

The Committee held 21 internal working meetings during the year. The matters considered in these meetings include matters of principle and related challenges, annual plans and budgets, plans and division of tasks relating to inspections, evaluation and follow-up of inspections, complaint cases, cases raised on the Committee's own initiative, media relations and other public relations, and participation in national and international meetings.

Both the Committee and the Secretariat attended many meetings in 2013. Some of the more important ones are briefly mentioned here. Meeting with the Norwegian Data Protection Authority on topics including the uncovering of American authorities' surveillance abroad, the implementation of the Police Register Act and the Norwegian Data Protection Authority's role as ombudsman in relation to PST. In September 2013, the Committee and the Secretariat took a study trip to Geneva and Strasbourg. In Geneva, the Committee organised a seminar in cooperation with the Geneva Centre for the Democratic Control of Armed Forces (DCAF) as part of the work on a handbook for oversight of international intelligence cooperation. The book, which is based on experience and research, will be published in 2014.

In Strasbourg, the Committee met with a representative of the secretariat of the Council of Europe's Committee of Experts on Terrorism (CODEXTER), the Norwegian judge on the European Court of Human Rights, and the Norwegian mission to the Council of Europe, among others. The purpose of these meetings was, among other things, to receive information about the Council of Europe's human rights and anti-terrorism work, and to discuss how the democratic oversight of international security and intelligence work can be improved.

In addition, both the chair and committee members have given lectures and talks about the Committee's work at seminars or meetings, including at Oslo Militære Samfund, the Norwegian Research Center for Computers and Law at the University of Oslo (*Personvernkonferansen*) and the Storting's newly elected Standing Committee on Scrutiny and Constitutional Affairs.

3.4 Proposal for an external evaluation of the Committee and expansion of the Secretariat

Since the EOS Committee was established in 1996, only minor amendments have been made to the law and directive that govern its activities. In the Committee's opinion, the oversight model is expedient. Nevertheless, the Committee endeavours to regularly evaluate and improve its activities within the applicable framework at all times. As described in the annual reports for 2011

and 2012, the Committee's framework conditions have changed considerably in many areas. Some of the changes involve expanding the powers and resources of the EOS services, the increasing cooperation between services at the national as well as international level, the technological complexity of the work etc. In recent years, surveillance in general and the EOS services in particular have attracted more attention, with emphasis e.g. on dilemmas relating to different types of civil protection and protection of privacy.

The Secretariat has been strengthened in recent years. This has resulted in better preparations for inspections, more cases being raised on the Committee's own initiative and the introduction of unannounced inspections. It has also enabled the Committee to work on some projects in greater depth – which has resulted in several special reports to the Storting.

The Standing Committee on Scrutiny and Constitutional Affairs' recommendation to the Committee's annual report for 2012 stated that the Committee has 'an independent responsibility for assessing how extensive oversight activities need to be in order to ensure satisfactory oversight of the secret services'. The Standing Committee also stated that 'in its budget proposals, the EOS Committee must take into consideration the possibility that more frequent oversight activities may become necessary in future in light of the expected rise in the secret services' level of activity'.

On this basis, the Committee asked the Storting in 2013 to consider an external future-oriented evaluation of its activity. The Storting's Presidium has informed the Committee that it wants such a review of the EOS Committee's work, including of the legal framework for its activities. The Committee has also asked the Storting for resources to further strengthen the Secretariat by adding three new positions: one legal adviser, one technologist and one social scientist.

4 THE NORWEGIAN POLICE SECURITY SERVICE (PST)

4.1 General information about the oversight

In 2013, the Committee conducted six inspections of the PST Headquarters (DSE). The Committee also inspected the PST entities in the districts of Troms, Sunnmøre, Søndre Buskerud and Østfold. The Committee receives briefings on the service's ongoing activities and about special topics and cases that the Committee has requested information about in advance in connection with inspections of both central and local entities. Specifically, investigation cases and prevention cases are reviewed and checked, as are the service's archives and registers.

In the annual report for 2012, the Committee stated that PST had processed large amounts of personal data and intelligence information outside archives and registers. Inspections in 2013 showed that this practice continued, also in other electronic folders that PST had not informed the Committee about.

As a result of information about the American authorities' surveillance abroad coming to light, the Committee was in 2013 informed of other states' intelligence activities in Norway and PST's cooperation with foreign services, including PST's procedures for information exchange. *The Committee will follow up oversight of PST's cooperation with foreign services in 2014.*

4.2 Inspection of archives and registers

Inspections of PST's electronic archives and registers are an important part of the Committee's oversight of the service. The necessity, specification of purpose, relevance and quality of information is subject to particular assessment.

It is also important to check that PST carries out individual assessments of the basis for registration, and that information in the intelligence register is deleted when the conditions for processing such information cease to exist. The oversight is based on random spot checks as well as more qualified and targeted searches. Before each PST inspection, the Secretariat conducts searches in the intelligence register Smart and other systems to which the Secretariat

has unrestricted access. The Committee reviews the results of the preparatory searches during the inspections. The Committee can conduct searches in the systems during inspections.

Examples of deletion

The Committee has raised several cases in 2013 where written questions have been submitted to PST regarding the processing of personal data in the service's archives and registers. *The Committee's impression is that, in all essentials, PST complies with the Committee's comments and agrees with the Committee's interpretation of the regulatory framework.* The Committee's inspections have therefore resulted in information about a number of persons being deleted from the service's systems. In one case, the Committee noted that PST had reduced its focus on a group in recent years, and that some of the registrations could therefore have been kept more up to date. On this basis, PST conducted a review of the group and another group that the Committee had raised questions about. *This led to the service deleting at least 89 persons from the Smart register.*

The five-year rule

It follows from Section 3-7 of the guidelines for PST's processing of information that '[i]ntelligence registrations to which no new information has been added after five years shall be reviewed' and that '[t]he information shall be deleted if it is no longer required for the purpose'.

In the annual report for 2012, the Committee referred to the fact that it had criticised PST for having practised exceptions from the five-year evaluation rule for certain categories of people without the Committee being aware of it. The PST discontinued the exception practice following a re-assessment. In 2013, the Committee has again noted and pointed out examples of persons belonging to the categories in question who have still not been re-assessed.

The Committee has also found several errors in the computer script that was supposed to give notification of a manual review of the five-year evaluation. As a result of these errors, a large number of persons have not be re-assessed. The Committee has pointed out that this is unsatisfactory. In one of the cases, PST stated that the correction of the above-mentioned computer script resulted in several thousand people being added to the five-year assessment list. The Committee consider these errors further examples of how the script intended to ensure that persons registered in Smart are re-assessed after five years has not functioned as intended.

4.3 Special report to the Storting about PST's registration of people affiliated to two Muslim groups

Section 15 of the PST Regulations prohibit the processing of information about a person 'based solely on what is known about the person's ethnicity or national background, political, religious or philosophical conviction' etc. In the annual report for 2010, the Committee reported that it had criticised PST for processing information about individuals' political or religious convictions in contravention of Section 15 of the PST Regulations. In follow-up, the Committee initiated a project to investigate PST's registration of persons affiliated to two selected Muslim groups. The Committee submitted a special report to the Storting on 24 April 2013.

The Committee's conclusions

1. In the Committee's opinion, PST initially had grounds for surveillance of key persons in the two groups in question. That is to say, it was necessary for preventive purposes in the counterterrorism field to form an impression of certain persons in the groups.
2. Nonetheless, PST had over time processed many pieces of information about persons in the groups that, in the Committee's opinion, did not appear to meet the necessity and relevance requirements in the PST Regulations Sections 13 and 14. The information in question included irrelevant information about key persons as well as information about more peripheral persons, the processing of information about whom did not seem to be relevant to PST's performance of its duties.
3. The service had also processed information about many persons in contravention of the PST Regulations Section 15 by registering information about them based solely on what was known about their religious convictions.
4. Several persons were mentioned in the intelligence register Smart in such a way that they were not or had not been reassessed and deleted pursuant to the five-year rule, for example because they had not

been established as separate person objects. PST lacked grounds for processing information about several of these persons, cf. the PST Regulations Section 13.

5. Indiscriminate collection and use of source information may be a contributory cause of the extensive registration practice discovered by the Committee during the course of its investigation.

Follow-up

During the Committee's work on the project, PST stated that, as a result of the Committee's investigation, the service recognised that it was necessary to examine its registrations in relation to the two groups in question. The internal review showed that the service had registered persons and processed information that was not necessary or relevant to PST's performance of its duties, some of it in contravention of the PST Regulations Section 15. PST took the findings seriously, and would consider additional internal follow-up measures.

The Standing Committee on Scrutiny and Constitutional Affairs submitted a unanimous recommendation on 4 June 2013. Both this recommendation and the subsequent consideration by the Storting on 10 June expressed broad support for the EOS Committee's conclusions. At the same time, PST was praised for having carried out its own investigations into the matter and implemented measures to remedy its own registration practice.

In October 2013, the Committee asked PST to give an account of the follow-up of the Committee's project report and its own internal review. In December 2013, the service stated in its letter of reply that its review of the two groups had resulted in the deletion of information about a total of 55 persons and 186 intelligence events from Smart. Information about another 28 persons had been changed. PST also stated that a new case processing procedure was drafted and distributed to managers at PST Headquarters and local entities for consultation with a deadline for submission of feedback in June 2013. The consultation round produced several adjustment proposals. The further process has been put on hold pending a better overview of what changes the future restructuring of PST will entail for the procedure. *The Committee takes a positive view of the fact that the service has prepared a draft new case processing procedure, and has requested that it be kept informed of the further process.*

4.4 Processing of information outside archives and registers

In the annual report for 2012, the Committee described PST's processing of information in what was called 'the I area'. The Committee was not aware of the use of this area, and it was inconsistent with the intention that no intelligence information shall be processed outside the intelligence register Smart, which PST had expressed on several occasions in its contact with the Committee. The Committee criticised PST for this practice. The case was followed up in 2013. The Committee's investigations have shown that information is still processed outside of the established archives and registers, and also in other electronic folders that PST has not informed the Committee about. However, the amount of such information turned out to be considerably greater than the Committee had discovered in 2012.

The following is an excerpt from the Committee's concluding letter to the service:

> 'Through several searches in the I area, the Committee has found very large amounts of information (...) including several Excel documents containing personal data about thousands of people. In the Committee's opinion, the documents appear to be searchable secondary registers, which PST is not supposed to have.
>
> This means that PST's use of the I area has been of a far more serious and intrusive nature than the Committee initially stated in its letter of 12 June 2012. This intensifies the Committee's criticism of PST in connection with the matter.'

As referred to in the annual report for 2012, PST decided to tidy up the I area. In June 2013, the Committee was informed that the review of the I area had been completed.

During its inspections of two local PST entities towards the end of 2013, the Committee nevertheless found that the entities were processing information in the I area. Furthermore, the Committee found, during its 2013 investigations of the service's computer network, that information has also been processed in another area in the folder structure – the F area. The findings include hundreds of photographs of persons, screenshots of personal Facebook profiles, lists of members of several organisations, and overviews of contact networks and relationships. On this basis, the Committee submitted several questions to PST in writing.

In its concluding letter to the service, the Committee stated the following:

> 'The Committee finds that it warrants criticism that the service has not informed the Committee about the use of the F area, which has in practice resulted in the information being withheld from the Committee's oversight, and that the Committee's conclusions in the I area case do not appear to have been followed up in relation to other corresponding areas. It is noted in this connection that several pieces of information processed in the F area were recent.'

4.5 PST's handling of communication between lawyers and clients in the I area

In connection with the Committee's investigation of PST's processing of documents in the I area, the Committee discovered that PST had processed a large amount of information stemming from confidential communication between lawyers and clients, most of which was obtained by means of communications control in cases under investigation. Several persons and their lawyers were affected. The Committee criticised the service for storing such strictly confidential information long after the cases were concluded. The material should have been deleted immediately. The Committee referred to the fact that communication between lawyers and clients enjoy special protection under the European Convention of Human Rights (ECHR) Article 8. Unwarranted storage of such communication constitutes a violation of the Convention's provisions. PST apologised to the Committee for having failed to delete such confidential communication between lawyers and clients obtained by means of covert coercive measures.

The Committee has been informed that PST has prepared a procedure for the processing of communication subject to special protection. The procedure states that such communication 'shall be deleted as soon as possible, if necessary after the police has reviewed the material to ascertain what should be deleted'.

4.6 PST's use of covert coercive measures

The Committee routinely conducts subsequent control of PST's use of covert coercive measures such as communications control, covert video surveillance, covert audio surveillance, technological tracking and secret searches. Pursuant to the Norwegian Criminal Procedure Act, PST can petition the courts for authorisation to use covert coercive measures in ordinary *investigations* and in order to *avert* certain criminal offences. PST can also, as the only police authority with this right, request the use of covert coercive measures to *prevent* certain types of serious criminal offences as mentioned in the Norwegian Police Act Section 17d. The Committee has noted that the use of coercive measures in preventive cases has increased in recent years.

Court permission

PST's use of covert coercive measures must be sanctioned by the courts. Persons subjected to covert coercive measures shall be represented by a 'secret lawyer', whose job it is to protect the interests of the person under surveillance during the court's consideration of PST's petitions for use of coercive measures. However, 'secret lawyers' have little possibility of following up their clients later as regards how the surveillance is carried out and its results. This makes the Committee's oversight of PST's subsequent use and implementation of coercive measures all the more important to the due process protection of persons under surveillance.

The Committee checks that the information provided to the court is correct. The Committee will in many cases have access to more information than the court has access to, including intelligence

information received from cooperating services both foreign and domestic. The Committee also conducts subsequent control to check that PST has used the coercive measures in accordance with the court's permission, for example that coercive measures have not been used for longer than the period stipulated by the court. In this connection, the Committee checks that PST's requests for assistance from telecommunications providers to carry out communications control are in accordance with the court rulings, see section 8.2 on the Committee's inspection of NetCom.

In 2013 the Committee criticised PST for errors in requests for assistance from telecommunications providers to carry out communications control that have in some cases resulted in the service exceeding the court's permission for use of coercive measures.

Covert audio and video surveillance

As regards covert audio and video surveillance, the Committee checks that the measures are used in accordance with any special conditions or intentions stipulated by the court etc. The Committee examines case logs to check the use of surveillance equipment, and actively checks whether the information provided to the court corresponds to what is actually under surveillance. It also receives image print-outs in cases where covert video surveillance has been initiated and compares them with the court rulings. *The oversight activities have not detected any covert video or audio surveillance by PST in contravention of court rulings.*

The Committee will endeavour to develop its oversight further in 2014, for example in relation to the service's internal logging of the use of technical equipment used in covert audio and video surveillance. This would enable the Committee to carry out more precise checks of such things as times of equipment installation and removal, and whether the service has the necessary internal control of its equipment.

4.7 PST's processing of applications for declassification and access

In its annual reports from 2007 to 2012, the Committee has described PST's processing of applications for declassification and access. The main question in the matter is whether individuals should be granted access to registered information about themselves that is more than 30 years old, alternatively access to the information that no information is registered about them. In several cases, PST has refused to grant individuals access to information that they were *not* registered in the service's registers 30 or more years ago.

In its recommendation to the annual report for 2009, the Standing Committee on Scrutiny and Constitutional Affairs stated that the question of permanent right of access should be considered. Shortly before the Standing Committee submitted its recommendation, the Storting adopted the Police Register Act, Section 66 of which states that no right of access shall apply to PST's archives and registers. At the same time, it was concluded that the Freedom of Information Act does not apply to the service. The question of access to old information was discussed on this basis in a meeting between representatives of the Committee and then Minister of Justice Knut Storberget in October 2010. It emerged that the Ministry was looking into the matter. The Committee then expressed its opinion regarding access to old information in a letter to the Ministry dated November 2010. The Committee wrote:

> 'Registration in PST's intelligence register or other surveillance activities constitute serious infringements on individuals' right to privacy. At the same time, it is very important to many people to clarify whether or not they have been registered by the service. (...) Access to old information is far less capable of causing harm to national security or the effectiveness of the service than access to more recent information. The service's operating methods and priorities will change over time, so that these considerations will in principle be a weaker argument the older the information in question is. In order to ensure that considerations of national security are safeguarded (...), regulations concerning right of access to old information can provide for certain exceptions.'

On this basis, the Committee concluded that statutory regulation should be introduced to provide for the possibility of individuals being granted right of access to old PST information. The Ministry

replied to the Committee's letter in December 2013, after many reminders. As regards the matter of classified information, the Ministry said:

> 'If all who are not registered were to be given confirmation that there is currently no information about them registered in PST's registers, that would implicitly mean that all who are *not* given such confirmation *are* in fact registered, and thus that the information processed is relevant to PST's performance of its duties at present. (...) For this reason alone, confirmation to applicants who are not registered would be very unfortunate for the service's ability to achieve its goals.'

The Committee took note of this. In its concluding letter to the Ministry, the Committee pointed out that it is still difficult to see why old information should be classified, including information that a person has *not* been registered, particularly considering the fact that the general rule in the Security Act Section 11 third paragraph is automatic declassification after 30 years at the latest.

The Committee will thus not get further in its work on matters relating to access to old information. The Committee put six complaint cases on hold pending clarification of the questions in the matter. The complainants will be informed that the Committee has concluded its work on the case.

4.8 Information exchange with cooperating foreign services

PST has legal authority to disclose personal data about Norwegian and foreign citizens to cooperating foreign services subject to certain conditions. The Committee regularly checks that PST complies with these conditions and the international human rights commitments by which Norway is bound. Among other things, the Committee checks which parties information is disclosed to, that the disclosure meets a defined purpose and that the consequences for individuals are proportionate to the purpose of the disclosure. The nature and quality of the information are also assessed. One important aspect of the Committee's oversight is to check that information is not disclosed to states that fail to respect human rights. The reason for this is that Norway is not to contribute directly or indirectly to human rights violations.

As a result of Edward Snowden's information about American surveillance abroad, the Committee has in 2013 asked whether information disclosed to cooperating services may have been used for unlawful surveillance of Norwegian citizens in Norway. Such investigations are demanding, as it is difficult for the Committee to check whether information is used by cooperating services in ways that contravene the conditions set by PST on its disclosure.

4.9 Persons with Norwegian connections registered in the Terrorist Screening Center's database

During an inspection of PST in April 2013, the Committee was informed that information about Norwegians had been processed in a database belonging to the Terrorist Screening Center (TSC), an FBI unit tasked with identifying suspected or potential terrorists. PST stated that it had entered information about a small number of Norwegian persons in the database. The criterion for entry was that the persons had been charged with or convicted of a criminal offence relevant to TSC's objective. PST can delete personal data that it has entered in the database if the information is not longer deemed to be relevant. Moreover, PST stated that information about many other persons with connections to Norway had been processed in the database, without the service knowing who had entered the names, the purpose of the processing and which party was the end user of the information. The service also stated that it has asked the US authorities about their processing of this information, but had received no reply.

Oversight challenges

Foreign services' intelligence and surveillance activities do not fall under the scope of the Committee's oversight responsibility. The Committee is tasked with uncovering and preventing any exercise of injustice against individuals in Norway, however. In the Committee's opinion, the fact that the American authorities are processing information about Norwegian citizens in the database could give cause for concern in relation to due process protection, since the information

has not been entered, approved or quality assured by PST. On this basis, the Committee sent a letter to the Ministry of Justice and Public Security in June 2013 requesting that the Ministry follow up the matter, if relevant by contacting the American authorities. The Ministry was also asked to consider requesting access to information about what type of information about Norwegian citizens not entered by PST has been processed. The purpose of this was to check that information had not been entered in the database in contravention of the limitations on the American authorities' activities in Norway and/or processed in contravention of the conditions that apply to the use of intelligence information belonging to PST.

A letter of reply from the Ministry of November 2013 refers to the fact that, due to the search criteria in the database, the actual number of registrations of Norwegian citizens or persons with connections to Norway was uncertain. It also emerged that, despite requests, PST has not been given access to complete lists. In addition, the service did not know on which basis TSC had entered persons in the database. The Ministry therefore assumed that TSC does not wish to grant the Norwegian authorities access to this information. The Ministry also wrote that this database belongs to the US authorities. Their entry of persons in this database could be based on information about Norwegian citizens obtained from open sources, via the USA's information collection in other countries, or via data about Norwegian citizens who are staying or have stayed in the USA or other countries that cooperate with TSC.

Status

The Committee subsequently sent a new letter to the Ministry, of which the following is an excerpt:

> 'The Committee is aware that after the Committee's letter of 19 June 2013, a meeting was held with representatives of the American authorities on the topic of American surveillance programmes for the purpose of clarifying facts, discussing dilemmas relating to the conflict between security concerns and concerns for protection of privacy (...) The Committee notes that the Ministry has found no reason to follow up the Committee's questions concerning the processing of information about [X] Norwegian persons in the Terrorist Screening Center (TSC) with the American authorities (...) On the basis of recent media stories about the uncovering of surveillance carried out by the American authorities etc., and the consequences processing in TSC could have for individuals, the Committee again urges the Ministry to consider whether to contact the American authorities to follow up the registrations, including the basis for processing the information, who entered the information, where the information originates from and what the purpose of the processing is.'

In its reply to the Committee, the Ministry stated that it would after all contact the American authorities in an expedient manner with a view to elucidating the matter as well as possible. *The Committee will follow up the matter in 2014.*

4.10 PST's role in connection with surveillance of Norwegians abroad by foreign services

In June 2013, the Committee concluded a case that raised questions about PST's role in connection with the surveillance of two Norwegians abroad. The surveillance was carried out by a foreign service.

PST contacted a cooperating service in the country in question because two persons involved in a case under investigation by PST were going abroad. One result of this contact was that the cooperating service conducted covert video surveillance of the suspects' hotel room during their stay in the country. Because covert video surveillance of hotel rooms is not permitted under Norwegian law, it was crucial to the Committee to clarify whether the method had been used on assignment for or at the request of PST. In such case, the method used might have to be evaluated in the same way as if PST itself had conducted the surveillance.

PST acknowledged that it could have specified in relation to the cooperating service that covert video surveillance of hotel rooms is not permitted under Norwegian law. PST also acknowledged to a certain extent that the measure was initiated on the basis of an initiative by PST, but not on

assignment for or at the request of the service. Therefore, PST could not see that the cooperation could be deemed to be in violation of the service's legal limitations.

In its concluding remarks to PST, the Committee stated the following:

> 'Following an overall assessment, the Committee has found there to be justified and significant doubts as to PST's role, particularly as regards the question of whether the video surveillance was carried out on assignment for or at the request of PST. In the Committee's opinion, this could involve circumvention of the legal limitations that apply to the service. In the circumstances, the Committee has found no grounds for criticism of PST's conduct in the matter, and will, after receiving the PST's account of the case, not pursue the matter further.'

In its future oversight of PST, the Committee will pay particular attention to the legal basis for cooperation with other services.

5. THE NATIONAL SECURITY AUTHORITY (NSM) AND OTHER SECURITY CLEARANCE AUTHORITIES

5.1 General information about the oversight

The Committee has carried out four inspections of NSM in 2013, including one inspection of the NorCERT department – the Norwegian Computer Emergency Response Team. During the year, the Committee has been given user access to the correspondence records system Public 360, which means that the Committee can conduct independent searches.

The inspections of the NSM headquarters primarily focus on personnel security. In addition, the Committee receives briefings and information about ongoing activities. During the reporting year, the Committee has reviewed all appeal cases concerning denials of security clearance that have been finally decided by NSM as *the appellate body*, as well as negative decisions that have not been complained against in cases where the NSM has made *initial security clearance decisions*. The Committee has also made spot checks of security clearance cases that have been dropped and of negative decisions that have not been complained against in cases decided by security clearance authorities other than NSM.

The Committee has been informed that serious cyberattacks represent a growing threat to Norwegian interests. During its inspections of NorCERT, the Committee focuses, among other things, on ensuring that the cooperation between the department and other intelligence, surveillance or security services takes place within the legal frameworks that govern the respective services, and that protection of privacy is safeguarded in NorCERT's performance of its activities. *The inspection of NorCERT in 2013 did not give grounds for follow-up.*

In 2013, the Committee was informed that several sectors have not identified sensitive objects within their area of responsibility in a satisfactory manner as required by the security legislation. This applies to the petroleum, finance and energy sectors in particular, as well as to satellite infrastructure. NSM has stated that, generally speaking, many are reluctant to comply with the Security Act.

Following the disclosure of information about the American authorities' surveillance abroad, the Committee has raised the following information security issues, among others, with NSM in writing: How does NSM work to raise awareness about secure internet use among Norwegian institutions? What, if anything, will NSM do to find out which Norwegian institutions etc. use computer programmes where foreign intelligence organisations may have planted weaknesses? Despite several reminders, NSM has not replied to the Committee's letter of 14 October 2013, in which the end of November 2013 was given as the deadline for replying.

Lacking and delayed response by NSM to the Committee's enquiries has been a general problem in 2013. In a letter to NSM of December 2013, the Committee expressed its opinion that the situation was most unsatisfactory, and that it expected it to improve significantly in 2014.

5.2 NSM's case processing in security clearance cases

In 2013, the Committee has focused on NSM's case processing times, the revision of the Security Act, personal history for closely related persons from other countries, the use of security interviews, and matters relating to equal treatment of applications by different security clearance authorities etc.

Case processing times

The Committee has noted that the case processing times in security clearance cases are often far too long, which was also pointed out in the annual reports for 2011 and 2012. This applies in particular to appeal cases and cases where NSM conducts vetting of personnel for other security clearance authorities. NSM has informed the Committee that the reasons for the long case processing times include the complexity of cases, an increase in the number of security clearance cases, vacancies and staff cutbacks. As regards processing of requests for access, NSM has also stated that the staff cutbacks necessitate prioritisation, and that access cases are not a top priority.

The Committee would like to point out that the issue of security clearance can be decisive for an individual's professional career, and that the processing of cases thus has a bearing on the options available to the persons concerned. Long case processing times could have negative consequences for individuals, for example in connection with appointments for positions and assignments abroad for which security clearance is a requirement. The time aspect is also very important to the requesting entities, for example in connection with staffing. The Committee would therefore like to emphasise the importance of maintaining satisfactory case processing times in security clearance cases. The present situation gives cause for concern.

The resource situation in the area of personnel security has also resulted in the Committee not receiving replies or receiving very delayed feedback from NSM in 2013. The Committee's consideration of appeal cases, for example, has suffered as a result of this. One example that serves to illustrate the situation is an appeal case where the Committee sent questions to NSM in late August 2013 with a deadline for responding set at the end of September 2013. NSM did not reply to the letter until February 2014.

Case processing procedures etc.

In 2013, the Committee was kept up to date about NSM's ongoing work on a new national personnel security tool to replace the case processing tool TUSS. The Committee expects the new national tool to contribute to faster and more efficient electronic case processing. NSM has stated that the new case processing tool will also include an experience base for security clearance authorities, which will contain internal grounds in appeal cases in anonymous form. But it takes time to enter cases in the database, and, according to NSM, this work is not a priority. As of November 2013, only six cases had been entered. *The Committee takes a positive view of the fact that NSM has established an experience database, and believes that this can ensure faster and better processing of security clearance cases in terms of information, equal treatment, use of security interviews etc.*

It was pointed out in the annual report for 2012 that several security clearance authorities conduct far fewer security interviews than envisaged in the Act, and that this is often due to a lack of resources. Failure to conduct security interviews can be a problem in relation to due process protection. *However, the Committee believes that security interviews can be conducted in a more flexible and less labour-intensive manner than is presently the case, and that this can lead to security interviews becoming more widely used.*

Personal history for foreign closely related persons
The Committee was informed in 2013 that NSM has prepared a circular that specifies the requirement for personal history for closely related persons in security clearance cases. The general rule is that the personal history for closely related persons must cover ten years. In practice, this means that, as a rule, closely related persons who come from countries with which Norway has no security cooperation must have lived in Norway for ten years. The circular was prepared because NSM has observed that practice in this field varies enormously. In the circular, NSM has stipulated a minimum limit for how far it is deemed justifiable to depart from the requirement. In any case, a concrete assessment must be carried out in each case of whether the requirement can be departed from. During the year, the Committee has raised several security clearance cases in which persons were denied security clearance because of their own or closely related persons' connections to other countries. The Committee has focused on information about the persons in question, observation periods when security clearance was denied and equal treatment, among other things.

Revision of the Security Act
NSM has also informed the Committee that work is under way to revise the Security Act, and that it is considering whether to submit a proposal to reduce the number of security clearance authorities. The Committee sees several advantages in such a proposal. For example, it could facilitate more experienced and competent security clearance authorities, which could contribute to improving due process protection, including equal treatment, and civil protection.

Security interviews
The Committee has questioned why NSM did not conduct security interviews in three security clearance cases where persons were denied security clearances on the basis of financial circumstances. It is stated in NSM's guidelines that 'its work is based on the understanding that security interviews shall be conducted in all cases where there is a possibility that security clearance can be denied on the basis of financial circumstances'. NSM wrote in its reply to the Committee that it was clearly unnecessary to conduct security interviews in the cases in question, among other things because the persons concerned have explained their situation either in writing or verbally over the phone. This has given NSM a sufficient basis for making a decision. The Committee commented on this as follows in its concluding letter to NSM:

> 'The Committee agrees that, in many cases, doubts can be resolved by more expedient means than a security interview. However, the Committee would like to underline that security interviews are an instrument for clearing up doubts and illuminating a case (...) In the Committee's opinion, considerations for the illumination of the facts of the case, the adversarial principle and the person in question's due process protection all indicate that one should consider whether some security interviews can be conducted in a less resource-intensive way by taking a flexible approach to the use of resources, scope etc.'

The Committee also noted that NSM believes the requirement for security interviews to be conducted in cases involving financial matters to be inexpedient. The NSM will therefore submit a request to the Ministry of Defence for permission to change the wording of the guide. *In the Committee's opinion, any changes to NSM's guidelines on this point should be clarified by the Ministry of Defence as soon as possible, considering that security interviews in cases involving financial matters are not practiced in accordance with the requirement set out in NSM's guidelines to Section 21 third paragraph.*

5.3 Differing practices between security clearance authorities
The Committee has also in 2013 seen examples of persons being granted NO CLEARANCE in connection with reclearance for SECRET level on the basis of connections to other countries, even though the basis for the assessment was the same as it was five years earlier, when the person in question was granted security clearance for SECRET level. The Committee has again

stated to NSM that such differences in practice give cause for concern in relation to security, but it is also a great burden on the person in question. NSM agreed with the Committee. The Committee questioned the stipulated observation period in the same case. The Committee and NSM agree that it is unfortunate when an observation period is set that does not reflect the actual possibility of being granted security clearance at the end of the period. NSM will follow up the issue in connection with consideration of appeal cases and supervision etc. *The Committee also pointed out that NSM has overriding responsibility for follow-up to ensure that the manner in which the regulatory framework is practised does not vary between security clearance authorities.*

5.4 Spot checks of security clearance cases in the Ministry of Transport and Communications

Three negative decisions made in security clearance cases from the Ministry of Transport and Communications that were not appealed were reviewed during the Committee's inspection of NSM in December 2012. In the cases in question, the Ministry made the decision NO CLEARANCE for three foreign citizens after receiving requests for security clearance from Telenor. The grounds given for the denials were inadequate personal history.

In a letter to the Ministry of June 2013, the Committee asked why the three persons in concerned had not been informed about and given grounds for the outcome etc. of their security clearance cases, and why no internal grounds were drawn up in the cases at the same time. *In its reply, the Ministry acknowledged that the information about and grounds for the decision had been sent to the requesting authority instead of to the persons concerned, and that this was done by mistake.*

5.5 Follow-up of inspection of the personnel security services at PST Headquarters/PST

The Committee carried out an inspection of the personnel security service at PST Headquarters in 2013. On the basis of this inspection and the service's briefings, the Committee submitted several questions concerning PST's personnel security work.

Security interviews

During the inspection, the personnel security service at PST Headquarters stated that the service did not conduct security interviews in accordance with the requirement in the Security Act Section 21 third paragraph, which stipulates that security interviews shall be conducted in cases where such an interview is not deemed to be obviously unnecessary. With reference to the fact that security interviews are an important tool for illuminating the case and help to promote the due process protection of individuals as well as national security, the Committee remarked that PST Headquarters' practice is not in accordance with the requirement for security interviews to be conducted. *When the case was concluded, PST informed the Committee that its practice will be tightened and that interviews will be conducted in accordance with the Security Act and NSM's guidelines.*

Preliminary investigation of applicants as part of the service's recruitment process

During the inspection, the service informed the Committee that preliminary investigation of the applicants is part of PST's recruitment process. This investigation includes searches in the Smart intelligence register and police registers. The personnel security service at PST Headquarters was asked to explain the legal basis for this practice. The Committee also asked whether the applicants consented to the service conducting such preliminary investigations.

On the basis of feedback from the service, the Committee remarked that the preliminary investigation appears to constitute an *informal vetting of personnel.* The purpose of the searches carried out by PST in its own (and the police's) registers seems to be to check whether the applicant is fit to hold security clearance, and it thus partly corresponds to PST's ordinary vetting of personnel in security clearance cases. The Committee referred to the fact that it follows from the Security Act Section 20 first and second paragraphs that '[v]etting of personnel shall be carried out at the request of the person responsible for authorisation, unless otherwise decided by the National Security Authority'. Vetting shall only take place once a security clearance is needed. The Committee remarked that consent is a condition for the security clearance authority

processing personal data about the person in question during vetting of personnel, including searches in PST/police registers.

In the Committee's opinion, PST has no legal authority pursuant to the PST Regulations Section 13 for processing information about applicants for positions in the service by conducting preliminary investigations or by processing information about the applicants by entering them in the Smart register on this basis. The Committee emphasised that PST's practice could weaken confidence in the security clearance authority.

On the basis of the Committee's comments, the service stated that this practice would be discontinued. The Committee also expected the service to review registrations of persons entered in the Smart register on this basis with a view to deleting them.

6. THE NORWEGIAN DEFENCE SECURITY AGENCY (FSA)

6.1 General information about the oversight

The Committee conducted three inspections of the FSA in 2013. During the inspections, the FSA has regularly given the Committee updates about its ongoing activities, including its protective security work, cooperation cases with other EOS services and the agency's personnel security and information security work. The Committee has unrestricted access to the FSA's internal case processing systems, which facilitates thorough oversight of the agency's activities.

The FSA is Norway's largest security clearance authority. Approximately 28,000 requests for security clearance were submitted in 2013. The FSA received about 17,000 of them, which corresponds to just over 60 per cent. The agency's processing of security clearance cases is therefore particularly important in the Committee's oversight of the FSA. The Committee reviews all negative security clearance decisions made by the FSA that have not been appealed, as well as new appealed security clearance cases where the agency granted the appeal in part or in full. The Committee also reviewed a large number of dropped cases in 2013.

During the inspection of Rena military base, the Committee was informed that the FSA's long case processing times in security clearance cases sometimes represent a challenge to Norwegian Armed Forces units, as clearance is a requirement for various positions or duties. The long case processing times can also result in soldiers' need for security clearance lapsing, for example because they are discharged.

The Committee requests regular updates about activities carried out by the FSA's office for activity and its underlying sections, including any training exercises, incidents, important cases and cooperation with other agencies or EOS services. The Committee also reviews spot checks relating to investigations of reported events that represent a threat to security, and operational cases conducted by the FSA as part of the agency's responsibility for military counterintelligence (Mil CI) in Norway in peacetime. *The review of these cases did not give grounds for further follow-up of the FSA in 2013.*

6.2 Cooperation between the FSA and PST

PST is responsible for counterintelligence and counterterrorism in Norway. The FSA can carry out military counterintelligence (Mil CI) operations, defined as identifying and counteracting activities that represent a threat to security in or in the immediate vicinity of military areas. The FSA shall share information with PST and inform PST of any suspicions of intelligence activities and sabotage etc. insofar as this is necessary. PST shall keep the FSA continually informed about circumstances with a bearing on military security and preparedness. The Committee has also in 2013 been kept up to date on the cooperation between the FSA and PST, including the work to prepare a cooperation agreement.

7. THE NORWEGIAN INTELLIGENCE SERVICE (NIS)

7.1 General information about the oversight

The Committee conducted six inspections of NIS in 2013. Two of the inspections were unannounced, see sections 7.2 and 8.4.

NIS is not permitted to monitor or in any other covert manner procure information about Norwegian legal persons on Norwegian territory. In its oversight of the service, the Committee maintains a particular focus on compliance with this prohibition. The legal position of Norwegian legal persons abroad is not regulated by the Intelligence Service Act. The service is nonetheless obliged to respect the provisions set out in the European Convention on Human Rights. This is also an important focus for the Committee's oversight.

Cooperation between NIS and PST has remained a priority oversight area for the Committee in 2013. In this connection, the Committee focuses in particular on ensuring that the services do no exceed their legal authority or areas of responsibility.

7.2 Special report to the Storting about NIS's archive of Norwegian sources

On 16 December 2013, the Committee submitted a special report to the Storting about its investigation into information about Norwegian NIS sources. To begin with, the Committee conducted one unannounced and one announced inspection of NIS's Section for human intelligence collection. The Committee reviewed all files on Norwegian sources in the section's archives and carried out several spot checks in its computer system.

The Committee's investigation did not find any indications that the service had systematically processed information about Norwegian sources and/or other Norwegian persons (potential sources and closely related persons of sources) in contravention of the applicable regulatory framework. Nor did the Committee find that the service had violated the prohibition on procuring information about Norwegian persons in Norway.

The Committee did, however, point out that NIS's legal basis for processing sensitive personal data about sources' closely related persons is questionable. The Committee also commented that it was difficult to see that the service can process other information about potential sources than what is necessary for documentation reasons, for future contact etc. The Committee was also of the opinion that the service had in some cases processed information that appeared irrelevant and/or unnecessary. On this basis, NIS was asked to follow up the need for a clearer legal authority for the processing of information about closely related persons of sources, and to prepare internal regulations for the use of sources. The Committee also called for clear rules concerning the collection and processing of information about potential sources. Finally, a condition was stipulated for the service's archives to be organised in such a way as to facilitate future oversight by the Committee. *In 2014, the Committee will follow up the clarification of the legal authority and the development of the service's internal regulations.*

7.3 The Committee's right to inspect NIS

Legal basis for the Committee's right of inspection/access

Pursuant to the Act relating to Oversight of Intelligence, Surveillance and Security Services Section 4 first paragraph, the Committee 'may demand access to the administration’s archives and registers, premises, and installations of all kinds' in pursuing its duties. 'All employees of the administration shall on request procure all materials, equipment, etc. that may have significance for effectuation of the inspection', cf. Section 4 second paragraph. Pursuant to the Act relating to the Oversight of Intelligence, Surveillance and Security Services Section 2 second paragraph, the Committee shall 'show consideration for national security and relations with foreign powers'.

It is stated in the Directive relating to Oversight of the Intelligence, Surveillance and Security Services Section 5 that the Committee 'shall not seek more extensive access to classified information than warranted by its oversight purposes'. The Committee is also obliged to

'insofar as possible' observe the concern for protection of sources and safeguarding of information received from abroad.

In the event of disagreement concerning the scope of the right of access, it is in principle up to the Committee to assess whether the considerations are sufficiently weighty for a service to deny access to information that the Committee requests. This is discussed on page 63 of Norwegian Official Report NOU 1994:4: 'The decision regarding the scope of access must necessarily be made by the oversight committee. However, these matters are of such importance that a formal right of objection should be put in place.' This was set out in the Directive relating to Oversight of the Intelligence, Surveillance and Security Services Section 6:

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

The Committee can then make a binding decision on the right of access and the scope of oversight. Any objections shall be included in the annual report, and it will be up to the Storting to express an opinion about the dispute, after the requested access has been granted (no suspensive effect).

Development in the Committee's right of inspection of NIS

In 1999, the Storting adopted a plenary decision for a special procedure to apply for disputes about access to NIS documents, *without amending the Act and Directive*. The Storting's 1999 decision was based on the particular sensitivity associated with NIS's sources, the identity of persons with roles in occupation preparedness and particularly sensitive information received from cooperating foreign services.

As a consequence of the Storting's decision, the Committee will have to submit NIS's refusal of access to the Minister of Defence, while also notifying the Storting. If the Minister finds that the Committee cannot be granted access, the case shall be brought before the Storting. Pursuant to this procedure, the Committee will not have access to disputed documents etc. until either the Minister of Defence or the Storting has decided that access is to be granted. In other words, objections made by NIS will have suspensive effect.

On this basis, the Committee has exercised caution in its oversight of NIS since 1999. Therefore, the service has only denied the Committee access to documents on a few occasions. The grounds for these refusals have been in accordance with the Storting's decision, and the Committee has so far not raised the matter with the Minister of Defence and the Storting.

'Particularly sensitive information'

In the annual report for 2012, the Committee stated that it was in dialogue with NIS to arrive at practical solutions for searching in the service's computer systems. The result of the dialogue is that the Committee should be able to search freely in the service's systems, with the exception that NIS will withhold information that the service deems to be 'particularly sensitive'. NIS defines 'information about Norwegian and foreign sources, persons in and operational plans for occupational preparedness, and a small number of particularly sensitive operations' as being 'particularly sensitive information'. Such information will be stored in separate areas in the computer network. The Committee will be kept informed about how many cases are withheld from the Committee's oversight and why.

The Committee finds the current situation challenging and believes that it gives cause for concern on grounds of principle, seen in light of the Committee's oversight responsibility and the right of access/inspection that follows from the Act and Directive relating to Oversight of the Intelligence, Surveillance and Security Services.

The Storting must clarify the right of access

In the Committee's opinion, it is important that the Storting as client clarifies the right of access in relation to NIS and how any disputes between the Committee and NIS should be resolved. Is it the Storting's intentions that the provisions in the Act and Direction should apply in full also to NIS? Or is the Storting's decision from 1999 to be upheld? If the latter is the case, the Committee feels that the Act and Directive relating to Oversight of the Intelligence, Surveillance and Security Services should be amended. This clarification will determine how extensive and thorough the EOS Committee can be in its oversight of NIS on behalf of the Storting.

The Committee would also like to point out that, generally speaking, NIS is concerned with demonstrating openness and trust through its briefings, presentation of collected intelligence information and facilitation of the Committee's oversight activities.

7.4 The Committee's oversight of the service's technical information collection

The Intelligence Service Act Section 4 first paragraph contains a prohibition against NIS monitoring or in any other covert manner procuring information concerning Norwegian persons on Norwegian territory. Effective oversight of this is contingent on the Committee being kept up to date about the technical systems and developments in collection methods. In 2013, the Committee was informed about the expansion of the service's exchange of information with selected partners, and about developments in the service's information collection methods. Oversight in this area is carried out on the basis of preparatory meetings between the service and the Committee Secretariat supported by a technical expert. In these meetings, briefings are given on the development of technical systems etc. This enables more efficient oversight by the Committee. *The Committee's oversight of the service's technical information collection has not resulted in criticism of NIS in 2013.*

The year 2013 was characterised by a focus on Norwegian citizens who travel to conflict areas abroad to take part in acts of war. NIS wrote in its unclassified assessment *Fokus 2013* that a conflict zone has developed in Syria that attracts persons from Norway who wish to fight the Syrian leadership. NIS expressed concern about several aspects of this development. As the Committee has previously pointed out, the service shall respect ECHR Article 8 concerning the right to privacy, also outside Norway. In 2013, the Ministry of Defence adopted provisions regarding collection of information relating to Norwegian persons outside Norwegian territory. In order for NIS to be allowed to monitor or in any other covert manner procure information concerning Norwegian persons abroad, the collection must take place as part of NIS's performance of statutory tasks, concern information that the service may lawfully hold and take place after interests of national security have been weighed against considerations for protection of privacy.

In 2014, the Committee will check that NIS's technical information collection is in accordance with the purpose of the Act relating to the Norwegian Intelligence Service, that the above-mentioned supplementary provisions are complied with, and that Norway's international obligations are observed.

7.5 Cooperation between NIS and PST

The Committee has also in 2013 focused on the cooperation between NIS and PST, particularly in relation to cooperation cases and exchange of information between the services. The basis for this cooperation is the fact that PST's area of responsibility covers what goes on within Norway's borders, while NIS's area of responsibility is outside the country. The services are required to cooperate in order to safeguard and protect the nation's interests. Cooperation must take place within the limitations imposed by the services' respective powers and areas of responsibility.

It is the Committee's impression that the services cooperate to an increasing extent. The Committee are given regular presentations of all new and concluded cooperation cases, including counterintelligence and counterterrorism cases. In addition to this, status is reported on for all ongoing cooperation cases. The Committee has also carried out several spot checks of the exchange of information between the two services.

The services, in cooperation with NSM, prepared their first coordinated threat and vulnerability assessment in 2013. The Committee was also informed about the establishment of a co-located counterterrorism centre to be led by the head of PST. *The Committee will monitor the issues raised by a partial co-location of PST and NIS resources, considering e.g. the material differences between their regulatory frameworks and areas of responsibility and the fact that each service is only permitted to obtain information in accordance with the legal basis that applies to it.*

In the annual report for 2011, the Committee pointed out that cooperation between PST and NIS in relation to persons who travel across national borders raises interesting matters of principle. In this connection, reference was made to the fact that while PST needs a court ruling to use intrusive methods, few material or procedural limitations apply to NIS's surveillance abroad. Since NIS has both a right and a duty to forward information of interest to PST, the Committee was of the opinion that this could mean that PST, via NIS, can gain access to methods that the service would not be entitled to use in relation to persons who leave Norway. During its oversight, the Committee has neither found any cases where the services have exceeded their areas of responsibility, nor any cases where one service has asked the other service to do so. *Nor has the Committee criticised NIS or PST for anything else to do with their cooperation in 2013. The Committee will continue to prioritise oversight of this area in 2014.*

7.6 Information exchange with cooperating foreign services

Pursuant to the Intelligence Service Act Section 3 second paragraph, NIS may establish and maintain intelligence cooperation with other countries. The exchange of information with cooperating services abroad is a precondition for and an important part of such cooperation.

How is the exchange overseen?

The Committee oversees NIS's exchange of information with foreign parties primarily by inspecting the service's communications system for information exchange with cooperating foreign services, and by keeping informed about the content of the NIS archives. Messages sent or responded to by NIS via this communications system, as well as reports published by NIS for its partners via the system, can be checked by the Committee. In 2013, the service has worked to improve the adaptation of logs from the system, which will facilitate the Committee's inspection of material that has been exchanged. The Committee has also been informed that a new form of data exchange is being developed that aims to ensure less and more targeted exchange, among other things. The service is working to make it possible for the Committee to inspect this system, and the work will probably be completed in 2014.

When NIS receives enquiries from cooperating services via the communication system, the service will examine the enquiry via its own systems. If information about Norwegian citizens emerges during this process, the information exchanged with cooperating services will be anonymised in order to prevent the identification of Norwegian citizens, unless the conditions for disclosing the information are met. The Committee checks that personal data are only disclosed to cooperating services after a concrete assessment in each individual case of whether there is a basis for disclosure. In this connection, the Committee also checks that NIS does not violate the above-mentioned prohibition on monitoring Norwegians on Norwegian territory.

More transparency

The Committee stated in its annual reports for 2011 and 2012 that NIS has prepared internal guidelines for the disclosure of personal data to foreign services. The guidelines were classified as RESTRICTED. In the annual report for 2012, the Committee expressed the opinion that freedom of information considerations dictate that such provisions should be unclassified. In summer 2013, unclassified supplementary provisions were adopted concerning NIS's collection of information relating to Norwegian persons abroad and the disclosure of personal data to cooperating foreign services. The provisions require personal data to be deemed to be necessary, and their disclosure must be weighed against the consequences for the person

concerned. Moreover, the information cannot be used as the basis for surveillance or other covert information collection relating to persons staying on Norwegian territory.

Human rights in partner countries
Like PST, NIS must also continuously assess the receiving state's attitudes to and respect for fundamental human rights when the service exchanges personal data or other information, including when information is shared as part of Norway's participation in international operations. As discussed in last year's annual report, NIS has prepared a set of instructions intended to reduce the risk of intelligence personnel contributing to torture or other inhumane or degrading treatment in relevant partner countries. The instructions are intended to set out a procedure to ensure management support and, if relevant, political support, in the most complex cases that involve a significant risk of contributing to human rights violations. These instructions entered into force on 1 January 2013.

In 2013, the Committee carried out searches and spot checks of messages that the service had sent to cooperating foreign services. As in previous years, the exchange of information with cooperating foreign services has been quite extensive, and the level of such exchange remains relatively stable. *On this point, the oversight has not given grounds for criticising the service in 2013.*

8 OVERSIGHT OF OTHER EOS SERVICES

8.1 General information about the oversight
The Committee continuously oversees the intelligence, surveillance and security services carried out by, under the control of or on behalf of public authorities. In other words, the oversight area is not linked to particular organisational entities, but is defined by function.

Pursuant to the Directive relating to Oversight of the Intelligence, Surveillance and Security Service, the Committee shall inspect at least two NIS units and/or intelligence/security service functions in military staffs and units. The Committee can also on its own initiative carry out inspections of other police entities and other agencies or institutions that assist PST, and otherwise such inspections as indicated by the purpose set out in the Act relating to the Oversight of Intelligence, Surveillance and Security Services. The inspections of NetCom, Rena military base and the Intelligence Battalion at Setermoen military base are briefly described below.

8.2 Inspection of NetCom
The Committee carried out an inspection of NetCom's police contact centre in October 2013. The centre assists PST and the ordinary police in connection with e.g. communications control, subject to the courts' permission.

During the inspection, the Committee carried out spot checks of the communications control implemented by NetCom on behalf of PST by permission of the courts. Later, the Committee carried out investigations in PST in connection with the same case. *The spot checks found no discrepancies between the permissions granted by the court and the communications control carried out in the cases in question.*

During the inspection, NetCom informed the Committee about challenges relating to security clearance of personnel that deal with communications control cases. The issue was also mentioned in the annual report for 2012 under the section on the inspection of Telenor. The Standing Committee on Scrutiny and Constitutional Affairs followed this up in its recommendation, in which it submitted the following proposal, which was adopted by the Storting in June: 'The Storting requests that the Government ensure that a security clearance requirement applies to persons who are directly involved in work for companies that assist in the performance of intelligence, surveillance, and security services.'

The Ministry of Defence subsequently stated in Proposition No 1 to the Storting (2013–2014) that it would clarify the scope of the Security Act in relation to the private enterprises in

question and look into to the possibility of simplifying the regulatory framework for security clearance of employees in such enterprises.

In 2014, the Committee will follow up the work relating to security classification of information in connection with assistance in carrying out communications control.

8.3 Inspection of Rena military base

The Committee inspected the intelligence and security functions at Rena military base in October 2013. The inspection focused primarily on the Telemark Battalion (TMBN) and the Norwegian Army Special Forces Command (FSK). The Committee also received a briefing from the operational support unit, including information about its security functions.

During the inspection, TMBN informed the Committee about the battalion's intelligence and security functions, including an account of the battalion's object security and personnel security functions.

At FSK, the Committee was briefed about the unit's organisation and mission, including the procedures and regulations that apply to its activities. The Committee was also informed about the unit's intelligence and security functions. The Committee inspected TMBN and FSK's electronic and physical archives relating to their security and intelligence functions.

8.4 Complaints against the Intelligence Battalion

In the annual report for 2012, the Committee described an unannounced inspection of the Intelligence Battalion at Setermoen military base. The grounds for the inspection was a complaint about surveillance and registration made by to journalists. On examination of the Intelligence Battalion's closed computer network, the Committee found information about the two complainants, including their names and photos and information about their education and work history. The Committee also found that the Intelligence Battalion had processed information about another seven journalists in their systems.

The Committee criticised the Intelligence Battalion for having processed the information about the journalists without legal authority and in violation of the Personal Data Act. The Committee also pointed out that it was very unfortunate if people are registered in the systems of the secret services based on their journalistic activities without a basis for registration existing. Based on the information uncovered, the Committee did not find that the Intelligence Battalion had planned or carried out any form of mapping or analysis of any of the journalists.

In principle, the Committee is bound by an unconditional duty of secrecy concerning its activities. The Committee is nevertheless to give unclassified statements to complainants and reports to the Storting. As a rule, the Committee will thus not inform parties other than the complainants and, if relevant, the Storting about the outcome of complaints cases. However, the Committee subsequently received complaints about the same matter from several other journalists. Because five of the nine journalists about whom the Intelligence Battalion had processed information had complained to the Committee and thereby been made aware of the Committee's findings in the case, the Committee decided, after carrying out a concrete assessment of the case, to make an exception from its duty of secrecy in the case. The Committee therefore sent a notification to the other four journalists about whom the Intelligence Battalion had processed information, but who had not filed complaints, in April 2013.

The Committee has since received three new complaints against the Intelligence Battalion. Based on this, the Committee conducted an unannounced inspection of the Battalion in May 2013. In addition, the Committee Secretariat carried out an unannounced investigation at Setermoen military base in September 2013. In connection with assertions made in one of the complaints, an unannounced inspection was also carried out of the NIS headquarters at Lutvann in August 2013. *The Committee's investigations found no evidence of further illegal activity or matters that warrant criticism on the part of the Intelligence Battalion.*