EOS COMMITTEE

NORWEGIAN PARLIAMENTARY OVERSIGHT COMMITTEE
ON INTELLIGENCE AND SECURITY SERVICES

ANNUAL REPORT 2016

Photo: Forsvaret

To the Storting

In accordance with Act No 7 of 3 February 1995 relating to the Oversight of Intelligence, Surveillance and Security Service (the Oversight Act) Section 8 subsection 2, the Committee hereby submits its report about its activities in 2016 to the Storting.

The annual report is unclassified, cf. the Oversight Act Section 8 subsection 2. Pursuant to the Act relating to Protective Security Service (the Security Act), the issuer decides whether or not information is classified. Before the report is submitted to the Storting, the Committee sends the relevant sections of the report text to each of the respective services for them to clarify whether the report complies with this requirement. The services have also been given the opportunity to check that there are no errors or misunderstandings in the factual descriptions.

Oslo, 15 February 2017

Eldbjørg Løwer
Eldbjørg Løwer

Svein Grønnern
Svein Grønnern

Theo Koritzinsky
Theo Koritzinsky

Øyvind Vaksdal
Øyvind Vaksdal

Håkon Haugli
Håkon Haugli

Inger Marie Sunde
Inger Marie Sunde

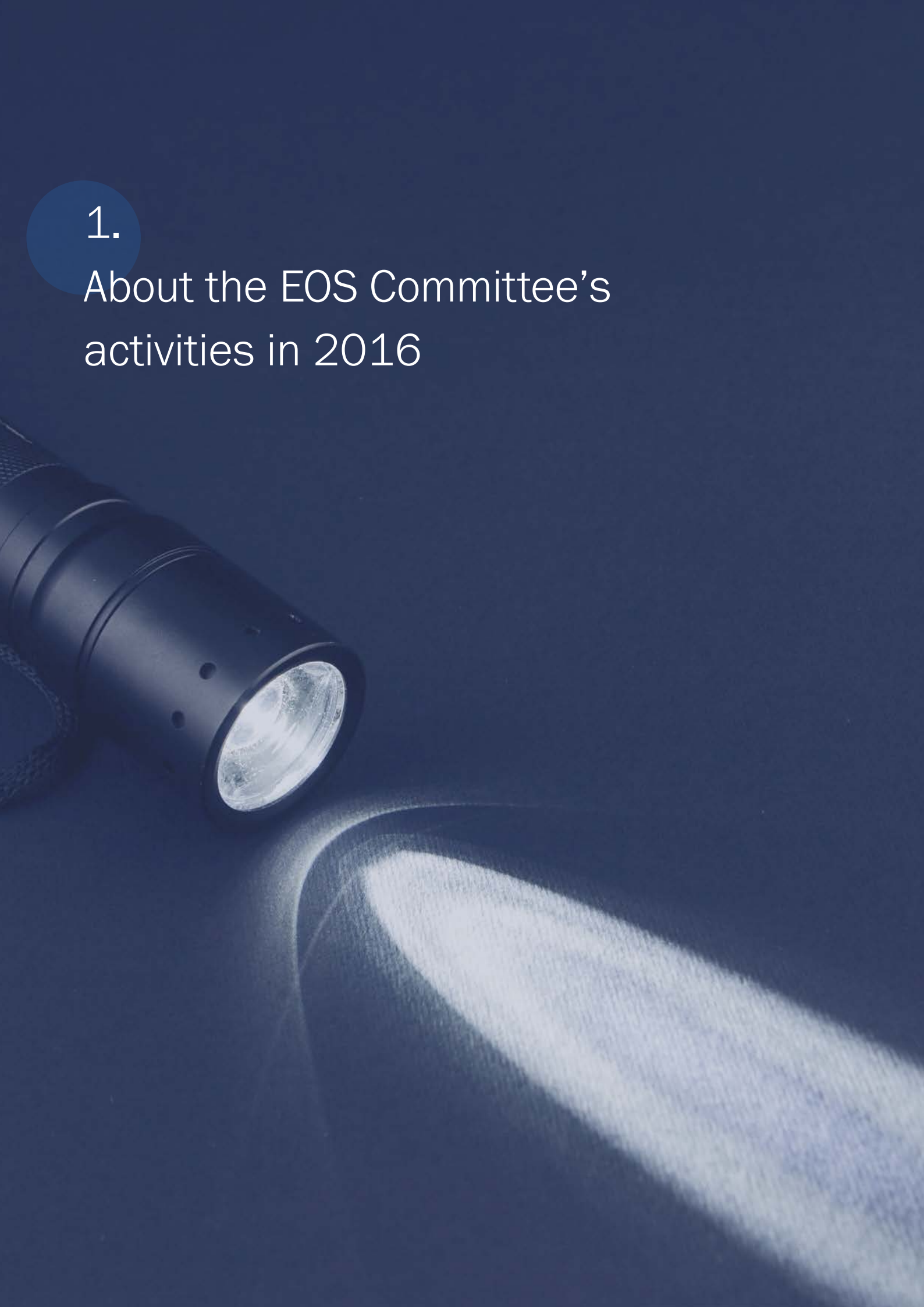
Eldfrid Øfsti Øvstedal
Eldfrid Øfsti Øvstedal

Henrik Magnusson
Henrik Magnusson

The Norwegian Parliamentary Intelligence Oversight Committee in 2017. Left to right: Theo Koritzinsky, Eldfrid Øfsti Øvstedal, Svein Grønnern (deputy chair), Eldbjørg Løwer (chair), Øyvind Vaksdal, Inger Marie Sunde and Håkon Haugli.

Contents

1.
About the EOS Committee's activities in 2016



1.1 The Committee's remit and composition

The EOS Committee is a permanent, Storting-appointed oversight body. The EOS Committee's task is to oversee all Norwegian entities that engage in intelligence, surveillance and security activities (EOS service. The Committee's remit follows from the Oversight Act and the Directive relating to Oversight of the Intelligence, Surveillance and Security Service[1] Only EOS servicecarried out by a public body or under the control of or on assignment for a public body are subject to oversight by the EOS Committee.[2]

Pursuant to the Oversight Act Section 2 first paragraph, the purpose of the oversight is:

1. to ascertain and prevent any exercise of injustice against any person, and to ensure that the means of intervention employed do not exceed those required under the circumstances, and that the services respect human rights,
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 in its oversight activities.[3] The Committee shall not seek more extensive access to classified information than warranted by its oversight purposes, and shall insofar as possible observe the concern for protection of sources and safeguarding of information received from abroad.[4] Subsequent oversight is practised in relation to individual cases and operations, but the Committee is entitled to be informed about the services' current activities. The Committee's oversight shall cause as little inconvenience as possible to the services' day-to-day operational activities.[5]

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.[6] 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 Committee has a broad composition so that both different political backgrounds and experience from other areas of society are represented. The committee members and secretariat employees must have top level security clearance and authorisation, both nationally and pursuant to treaties to which Norway is a signatory.[7] This means security clearance and authorisation for TOP SECRET and COSMIC TOP SECRET, respectively. Below is a list of the committee members and their respective terms of office:

Eldbjørg Løwer, Kongsberg, chair
1 July 2011 – 30 June 2019

Svein Grønnern, Oslo, deputy chair
13 June 1996 – 30 June 2021

Trygve Harvold, Oslo
7 November 2003 – 30 June 2016

Theo Koritzinsky, Oslo
24 May 2007 – 30 June 2019

Håkon Haugli, Oslo
1 January 2014 – 30 June 2021

Øyvind Vaksdal, Karmøy
1 January 2014 – 30 June 2021

Inger Marie Sunde, Bærum
1 July 2014 – 30 June 2019

Eldfrid Øfsti Øvstedal, Trondheim
1 July 2016 – 30 June 2021

Of the seven committee members, five have political backgrounds from different parties. This helps to strengthen the Committee's legitimacy.

1 Act No 7 of 3 February 1995 relating to the Oversight of Intelligence, Surveillance and Security Services (the Oversight Act) and Directive No 4295 relating to Oversight of the Intelligence, Surveillance and Security Service, adopted by a Storting resolution on 30 May 1995. The Act and Directive were most recently amended in May 2016.

2 References to the Oversight Act are found in Act No 10 of 20 March 1998 relating to Protective Security Service (the Security Act) Section 30, Act No 11 of 20 March 1998 relating to the Norwegian Intelligence Service (the Intelligence Service Act) Section 6, Instructions No 695 of 29 April 2010 for Norwegian Defence Security Department Section 14, and Act No 16 of 28 May 2010 regarding Processing of Information by the Police and Prosecuting Authority (the Police Register Act) Section 68.

3 Cf. the Oversight Act Section 2 second paragraph.

4 Cf. the Directive relating to Oversight of the Intelligence, Surveillance and Security Service Section 5 first paragraph. It is stated in the Directive relating to Oversight of the Intelligence, Surveillance and Security Service Section 6 that the Committee can make binding decisions regarding right of access and the scope and extent 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). In 1999, the Storting adopted a plenary decision for a special procedure to apply for disputes about access to National Intelligence Service documents.

5 Cf. the Directive relating to Oversight of the Intelligence, Surveillance and Security Service Sections 4 and 7.

6 Cf. the Directive relating to Oversight of the Intelligence, Surveillance and Security Service Section 1 first paragraph.

7 Cf. the Directive relating to Oversight of the Intelligence, Surveillance and Security Service Section 1 second paragraph.

The Committee is supported by a secretariat, currently consisting of eleven employees. At year end 2016, the Committee Secretariat comprised the head of the secretariat, who has a law degree, six legal advisers, one adviser in social sciences, one technological adviser and two administrative advisers.

1.2 Oversight activities carried out

The Committee's oversight activities mostly take the form of announced inspections of the EOS services. The Directive relating to Oversight of the Intelligence, Surveillance and Security Servicerequires the Committee to carry out at least 23 inspections per year.[8] In 2016, the Committee conducted 26 inspections. The Norwegian Police Security Service (PST) was inspected ten times, the Norwegian Intelligence Service (NIS) five times, the National Security Authority (NSM) four times and the Norwegian Defence Security Department (FSA) three times. The personnel security service of the National Police Directorate and the County Governor of Rogaland and intelligence and security functions at the Royal Norwegian Navy's main base (Haakonsvern) and the Norwegian Armed Forces' Joint Headquarters (NJHQ) were also inspected.

In the annual report for 2015, the Committee gave a more detailed description of the two parts that make up its inspections. The Committee has noted that the Standing Committee on Scrutiny and Constitutional Affairs expressed in its recommendation to the Storting that this is an expedient division.[9] The Committee has continued this practice in 2016.

In order to ensure that the Committee's oversight is targeted and effective, the Secretariat conducts thorough preparations in relation to the services. The preparations have been continuously strengthened over the past ten years. Inspections are scheduled in meetings between the Committee Secretariat and contact persons in the services, and then confirmed in an inspection letter sent before the inspection takes place. Preparation for inspections is a resource-intensive part of the Secretariat's activities.

The Committee can carry out most of its inspections *directly in the services' electronic systems*. This means that the inspections contain considerable unannounced elements. This reduced the need for unannounced inspections in 2016.

The Evaluation Committee's chair Bjørn Solbakken presents the Evaluation Report to the President of the Storting Olemic Thommessen 29 February 2016. Photo: Terje Bendiksby / NTB scanpix

The Committee raised 51 cases on its own initiative in 2016, compared with 37 cases in 2015. The cases raised by the Committee on its own initiative are mostly follow-up of findings made during its inspections.

The Committee investigates complaints from individuals and organisations. In 2016, the Committee received 32[10] complaints against the EOS services, compared with 23 complaints in 2015. The Committee prioritises the processing of complaints, and uses more and more resources in this field. The Committee dismissed some complaints on formal grounds, among other things because they did not fall within the Committee's oversight area. Complaints and enquiries that fall within the Committee's oversight area are investigated in the service or services that the complaint concerns. Generally speaking, the Committee's practice is to have a low threshold for considering complaints.

The committee members meet every month, except in July. Each member spends about four days on work relating to each meeting cycle, including reviewing case documents before the Committee's meetings and inspections. In 2016, the Committee had twelve internal full-day meetings at its office, in addition to several working meetings on site in connection with inspections. At these meetings, the Committee discusses planned and completed inspections and considers complaints and cases raised on the Committee's own initiative.

The EOS services have generally demonstrated understanding of the Committee's oversight in 2016, as in previous years. Experience shows that the oversight helps to safeguard individuals' due process protection and to create public confidence that the services operate within their statutory framework.

1.3 External evaluation of the EOS Committee

As described in previous annual reports, the Presidium of the Storting appointed a Committee on 27 March 2014 chaired by then Senior Presiding Court of Appeal Judge Bjørn Solbakken. The Evaluation Committee was tasked with evaluating the EOS Committee's activities and framework conditions. The basis for this was that the Committee had noted a development over time in the intelligence, surveillance and security field that had consequences for the Committee's statutory oversight duties, and it therefore proposed an external forward-looking evaluation of its activities.

The Evaluation Committee submitted its report to the Storting on 29 February 2016.[11] The Standing Committee on Scrutiny and Constitutional Affairs' recommendation to the Storting was submitted on 15 December 2016.[12] It is stated in the recommendation that representatives on the committee will submit a proposal for amendment of the Oversight Act to the Storting in the form of a private member's motion. The Evaluation Committee's proposals for amendment will then be considered in more detail. The EOS Committee looks forward to the Storting's further consideration of the case.

The EOS Committee has also noted the Storting's other comments to the evaluation report and will base its oversight activities on them in the time ahead. Particular reference is made to the Storting's statement that the EOS Committee itself should take steps to 'rationalise case processing, reduce the number of full-day meetings and make better use of the Secretariat's expertise and capacity'.

The EOS Committee assesses its work methods on a continuous basis, and all routine oversight duties have been delegated to the Secretariat. This allows the Committee to give priority to cases and issues that concern important matters of principle. At the same time, such steps will make it possible to continue to combine the office of committee member with participation in the ordinary labour market, which the Storting has emphasised is important. The Committee shares the Storting's opinion.

The EOS Committee will take account of the Storting's comments at all times. In 2017, the Committee will start a systematic assessment of which oversight duties can be delegated to the Secretariat in order to meet the Storting's wish for more efficient case processing and a reduction in the number of full-day meetings.

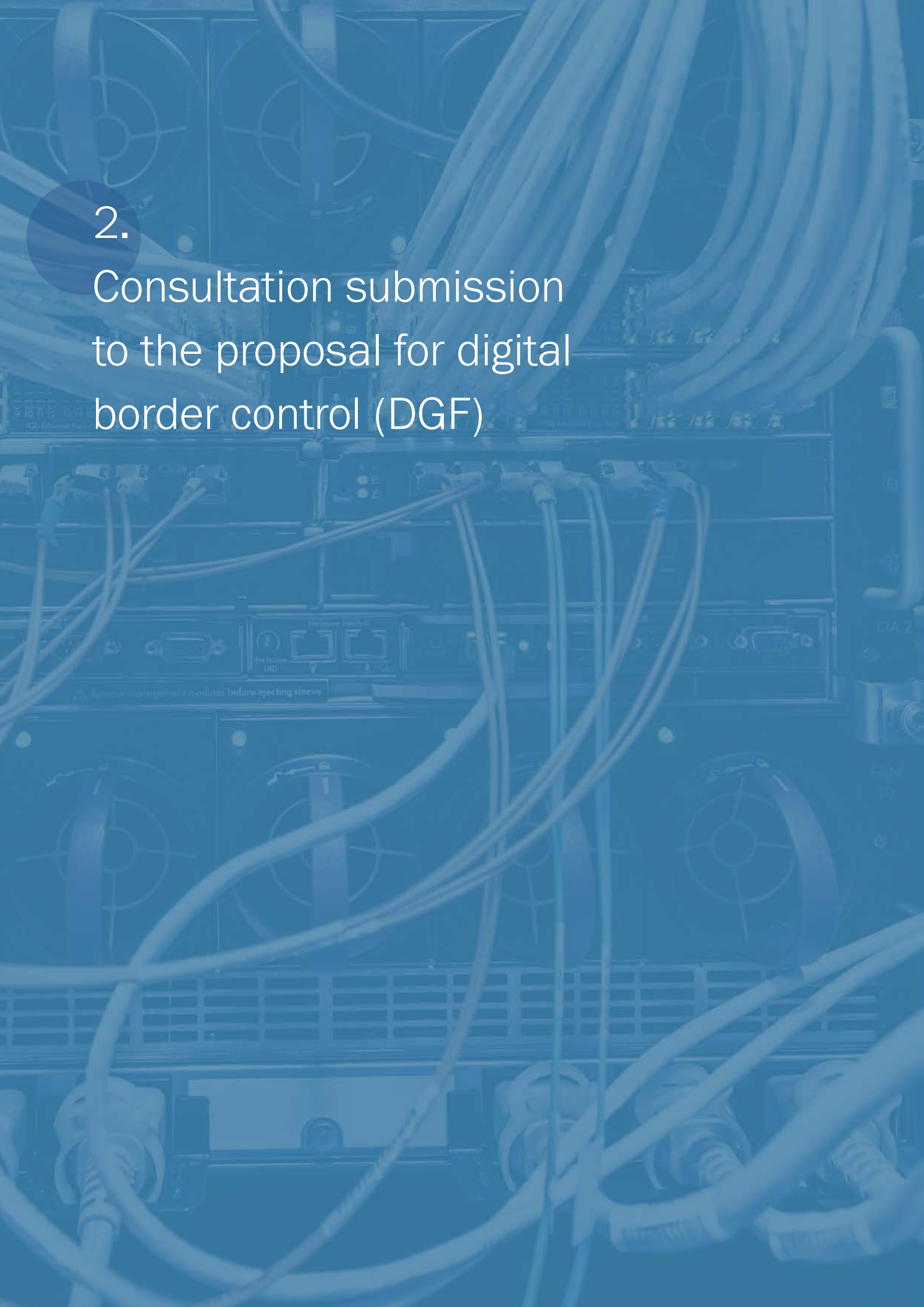
8 Cf. the Directive relating to Oversight of the Intelligence, Surveillance and Security Service Section 11 subsection 2.

9 Recommendation No 145 to the Storting – 2016–2017.

10 Some complaints concern more than one of the services.

11 *Report to the Storting from the Evaluation Committee for the Norwegian Parliamentary Intelligence Oversight Committee*, Document 16 (2015–2016).

12 Recommendation No 146 to the Storting (2016–2017).



2.
Consultation submission to the proposal for digital border control (DGF)

On 5 October 2016, the EOS Committee received the Ministry of Defence's *Report by the Lysne II Committee on digital border control (DGF) for consultation*.

It has been the EOS Committee's practice to have a high threshold for submitting consultation statements concerning proposals for new methods for the EOS services. The Committee nevertheless feels that it is important to submit a statement in cases where such proposals will have direct consequences for the EOS Committee's oversight and/or if there are e.g. circumstances that the Committee feels should be known before the Storting considers a bill.

It is not for the EOS Committee to have an opinion about whether or not digital border control should be introduced in Norway. However, the Lysne II Committee's proposal could have tangible consequences for the Committee's oversight activities should digital border control as outlined in the proposal become a reality. Due to the complexity and organisation of the proposed oversight functions, of which it is proposed that EOS Committee should constitute an important part, the Committee saw reason to submit a consultation statement on 20 December 2016 regarding the Ministry's proposal to introduce digital border control. In particular, the EOS Committee has opinions about the proposal to establish a separate DGF supervisory body and the challenges this will represent in relation to the Committee's parliamentary oversight of the Norwegian Intelligence Service and the proposed method. The consultation submission is enclosed as Appendix 5 to this report.

The EOS Committee has been in contact with the Swedish inspection authority for military intelligence activities (Statens inspektion för försvarsunderrättelseverksamheten, abbreviated SIUN) for several years. Among other things, SIUN oversees compliance with methods allowed under the Swedish signals intelligence act (the FRA Act), which regulates the Swedish National Defence Radio Establishment's (FRA) collection of signals from all types of signal carriers, not only signals transmitted via cables. The Committee intends to develop this contact further, and is planning to visit SIUN in 2017.

3.
Twenty years of parliamentary oversight of the EOS Services

Photo: Torgeir Haugaard / Forsvaret

The year 2016 marked the first twenty years of parliamentary oversight of the EOS services by the EOS Committee. The Committee has presented the results of its oversight activities in its annual reports and special reports, and they show that there is no doubt that a clear need for democratic reviews of the legality of these services has existed and continues to exist. The matters warranting criticism that the Committee has identified are often due to system errors rather than intentional acts on the part of individual employees, parts of the services or the service's leadership. Statistics for the period 1996–2016 are reproduced in Appendix 6 to this report.

The EOS Committee's most important oversight task is to ensure that the EOS services do not act in a manner that interferes with the rights of individuals to a greater extent than the legal rules permit. The Committee is charged with ensuring that the means of intervention employed do not exceed those required under the circumstances and that the activities do not involve undue damage to civic life.[13] The services must balance considerations for individuals' right to privacy against society's and thus all citizens' need for security. It is a demanding part of the services' work to strike this balance, and it represents a challenge from an oversight perspective. It is the Committee's duty to take a critical approach to the services' actions, while the services must be able to utilise the freedom of action that the legal framework provides.

The EOS services are subject to a detailed regulatory framework relating to the protection of privacy, and appear to focus on due process protection. Considerations of individuals' due process protection and protection of privacy form part of the services' basis for assessment when considering whether to use different forms of covert surveillance measures. The Committee considers it a clear advantage that Norway has organised oversight in such a way that one body exercises democratic oversight of all the EOS services. In a time of increasing cooperation between services, particularly between NIS and PST in their counterterrorism efforts, this factor is crucial to being able to carry out comprehensive oversight.

Although the EOS services have become considerably more open about their activities and the threat situation facing Norway and Norwegian interests, citizens who are under surveillance have no access to information about the services' surveillance. Whether or not the services have information about a person is in itself still classified information. The Committee can therefore only inform complainants about whether or not their complaint gave grounds for criticism. From the complainant's point of view, such an answer is often not very informative. In connection with individual cases, the Committee has raised with the ministry in question the possibility of giving the complainant a more comprehensive explanation.

The rapid technological development means that both the threat situation and the EOS services' methods are changing. New forms of communication provide new opportunities, both for government organisations and for parties not associated with any state, to carry out intelligence activities, attacks against Norwegian interests and acts of terrorism. The EOS services must counteract the cyber threat by continuously developing new tools and methods. The amounts of data that the services hold and the complexity of their computer systems and surveillance measures are increasing all the time. There is reason to believe that we have only seen the beginning of this development. The use of e.g. big data, sensors and artificial intelligence can give us surveillance and security services that are completely different from what we know today. The Committee has to adapt its oversight activities to the technological development. The Committee has had access to an external technical expert for a long time. In 2016, the Storting appointed the first committee member with a professional background in technology, and the Committee appointed the first technologist to its secretariat. The Committee is of the opinion that it will be necessary to strengthen its technological capacity over time.

If digital border control (DGF) is introduced, the Committee's need for technological expertise will increase. PST's right to read information in a computer system that is not publicly accessible, a method which was enshrined in law in 2016, is also part of this development. How to handle surplus information, use of big data and various issues relating to 'deleting' information represent important challenges both to the services and to the Committee's oversight.

13 Cf. the Oversight Act Section 2.

4.
The Norwegian Police Security Service (PST)

4.1 General information about the oversight

In 2016, the Committee conducted six inspections of the PST Headquarters (DSE). The Committee also inspected the PST entities in Sør-Trøndelag, Vestfold, Nordland and Southwest police districts.

In its inspections of the service, the Committee focuses on the following in particular:

- The service's processing of personal data (registration of persons)
- The service's new and concluded prevention cases and investigation cases. All ongoing prevention and investigation cases are reviewed every six months.
- The service's use of covert coercive measures (for example wiretapping and covert audio surveillance)
- The service's exchange of information with foreign and domestic partners.

During its inspections, the Committee is regularly informed about PST's ongoing activities, including the service's new prevention and investigation cases, threat assessments, and the service's cooperation with other EOS services.

In 2016, as in previous years, the Committee has focused on the cooperation between PST and NIS, particularly in relation to cooperation cases and exchange of information between the services.

In 2016, the Committee asked to be informed about the service's non-conformity reporting. PST found that the service's own non-conformity reporting system was unsatisfactory for non-conformities relating to the processing of personal data. PST informed the Committee that a new system for handling non-conformities will be introduced. The Committee will follow up PST's non-conformity system in 2017.

The Committee carries out oversight activities in relation to paper archives during its inspection of local PST entities. In 2016, the Committee raised a question about the finding of a document that had no relevance to PST's work. It turned out that PST was storing the document on behalf of the police district. The service will ensure that the formal requirements that apply to such storage are addressed in future (data processor agreement[14]). The Committee took note of the service's statement.

4.2 PST's unwarranted processing of confidential lawyer-client and doctor-patient communication

During an inspection of the PST Headquarters in April 2015, the Committee carried out oversight activities in relation to PST's communications control system. The Committee conducted targeted searches for communication that enjoys special protection under the Criminal Procedure Act. These searches showed that PST stored 38 conversations that were confidential and protected conversations between lawyers and clients and between doctors and patients. The committee members listened to some of these conversations.

In principle, wiretapping of confidential communication by the police is not prohibited, but this communication enjoys special protection that is regulated in more detail in the Criminal Procedure Act. In the same way as the courts cannot receive statements from lawyers, doctors etc. about 'anything that has been confided to them in their official capacity',[15] the prosecuting authority is obliged to 'as soon as possible'[16] destroy recordings or notes from communications control about such issues.

The conversations subject to the Committee's oversight had been recorded in the period from September 2009 to February 2015. The Committee stated in its concluding statement to PST in 2016 that the service should have destroyed these conversations 'as soon as possible', and that the Committee therefore found that it clearly warranted criticism that PST was still storing them in its system at the time of the Committee's inspection in April 2015. The Committee made the following statement when the case was concluded:

> 'The Committee finds that the 38 conversations, obtained by PST through communications control in the period from September 2009 to February 2015 and specified in the appendix to the Committee's letter of 10 June 2015, are mostly confidential and protected lawyer-client and doctor-patient conversations, cf. the

14 A data processor agreement is an agreement between the party responsible for the data (known as the *data controller*) and the party that processes data on behalf of the data controller (known as the *processor*), cf. the Personal Data Act Sections 13, cf. 2. A processor may not process personal data in any way other than that which is agreed in writing with the controller, cf. the Personal Data Act Section 15.

15 The Criminal Procedure Act Section 119 first paragraph reads as follows: 'Without the consent of the person entitled to the preservation of secrecy, the court may not receive any statement from clergymen in the state church, priests or pastors in registered religious communities, lawyers, defence counsel in criminal cases, conciliators in matrimonial cases, medical practitioners, psychologists, chemists, midwives or nurses about anything that has been confided to them in their official capacity.'

16 The Criminal Procedure Act Section 216 g letter b) reads as follows: 'The prosecuting authority shall ensure that recordings or notes made during communication control shall as soon as possible be destroyed in so far as they (...) relate to statements concerning which the court may not pursuant to the provisions of sections 117 to 120 and 122 require the person concerned to testify, unless the said person is suspected of a criminal act that might have provided independent grounds for control.'

Criminal Procedure Act Section 119. The Committee is therefore of the opinion that the service should have destroyed these conversations 'as soon as possible', cf. the Criminal Procedure Act Section 216 g letter b), and thus finds that it clearly warrants criticism that PST still processed (stored) these conversations (...) at the time of the Committee's inspection in April 2015.
(...)
PST wrote in a comment to conversation number 19 in the service's letter of 29 January 2016, cf. the appendix to the Committee's letter of 10 June 2015, that '[t]he conversation was not deleted because it was not perceived to be a lawyer-client conversation'. In connection with the Committee's inspection the following was noted from the service's summary (...) concerning the conversation in question: '[Person] calls [person] and talks about the court case'. In the Committee's opinion, the service's summary indicates that this also constitutes protected and confidential lawyer-client communication. PST is therefore also criticised for not having destroyed this conversation earlier in accordance with the Criminal Procedure Act Section 216 g.

The Committee notes that PST considers it highly regrettable that this type of conversation was found in [the service], and that all the conversations have now been or will be deleted. This suggests to the Committee that the service has already taken on board the essence of the Committee's statement. This is positive.'

4.3 Failure to conduct reviews under the five-year rule

4.3.1 Background

An important part of the Committee's inspections of PST is the oversight of the service's intelligence register Smart. Intelligence registrations to which no new information has been added after five years shall be reviewed by the service, cf. the Police Register Regulations Section 22-3 third paragraph. The information shall be deleted if it is no longer required for the purpose. In one case, the Committee questioned why information had not been reviewed despite no new information being added for more than five years.

4.3.2 The criterion 'new information'

The most recent information about one person had been added in 2009, but the person in question was mentioned in a threat assessment in a log from 2012. The information about the person had not been reviewed. The Committee questioned the interpretation of the criterion 'new information' and what criteria form the basis for interrupting the time limit under the five-year rule. PST stated that in order for the time limit to be interrupted, the service must receive new information that was not previously known and that is deemed relevant to the performance of the service's duties. Smart's technical design meant that other registrations, including the log entry, interrupted the time limit. The service was aware of the unfortunate consequences of this, and had changed the criteria for triggering an interruption so that the

most recent registered intelligence event forms the basis for calculating the five-year period. PST noted that, due to resource considerations, the change was not given retroactive effect, so that information about approx. 100 persons will not be reviewed until five years after the last registration. The information about the person whom the Committee asked about fell into this category, and the information was deleted.

The Committee agreed with the service's interpretation of the term 'new information' and noted that as many as 100 persons were not covered by the changes to Smart's computer script[17] due to resource considerations. The Committee issued a general reminder that resource considerations and any technical weaknesses in computer solutions do not relieve PST of the obligation to comply with the applicable regulatory framework.

4.3.3 Review of information about legal persons

Relating to the registration of an enterprise, PST stated in its reply that the computer script is not adapted for reviews of organisations. The Committee pointed out that 'registered' in the Police Register Act Section 2(6) covers both physical and legal persons, and that the requirement for review stipulated in Section 22-3 third paragraph of the Regulations is not limited to personal data. PST agreed with the Committee that the requirement also applies to legal persons, and stated that the service will look into the possibility of including legal persons in the computer script for review under the five-year rule. The Committee stated that it should be possible to make such a change.

Since the Committee made its concluding statement, PST has referred to technical challenges relating to compliance with the regulatory requirements for review of information, but that the service will look into possibilities for changing its practice. The Committee expects the matter pointed out to be remedied shortly, and will follow up the matter in 2017.

4.4 Registration of information about persons who have been suspects in criminal cases

In one case, the Committee asked PST about why intelligence registrations relating to one person had not been reviewed in accordance with the five-year rule, cf. the Police Register Regulations Section 22-3 third paragraph. PST referred to the fact that the person had been involved in an investigation case and stated that the Police Register Act's provisions concerning deletion and restriction of access to information[18] do not apply to 'information in criminal case documents'. The Committee asked whether it was the service's view that all information registered in Smart about persons who have been suspects in an investigation case is covered by the term 'criminal case documents' in the Police Register Regulations Section 25-2.

PST stated that this term is subject to extensive case law, and referred to how, under current law, the documents in the case cover 'almost any document produced during an investigation'. The Committee understood the service's view to be that all intelligence registrations in Smart relating to objects who have been suspects in an investigation case are exempt from the requirement for review after five years, since they constitute 'information in criminal case documents'.

When concluding the case, the Committee made the following statement:

> 'The Committee disagrees with PST's interpretation of the regulatory framework. The Committee cannot see that intelligence registrations in Smart containing information about persons who have been suspects in investigation cases are exempt from the requirement for review in accordance with the five-year rule. As the Committee understands PST's interpretation of the regulations, it would mean that intelligence registrations relating to objects who have been involved in an investigation case shall never be reviewed for deletion. The Committee considers it unlikely that this was the legislators' intention. Reference is made to the fact that the exemption from deletion and restriction of access to information in the Police Register Regulations Section 25-2 relates to "criminal case documents", and not to "intelligence registrations" pursuant to the Police Register Regulations Section 22-3 third paragraph. In the Committee's opinion, one must therefore distinguish between information logged in an investigation case, which must be considered "criminal case documents", and the intelligence information that is included in intelligence registrations in Smart.
>
> The Committee's statement contains a request that PST change its practice, and the Committee requests feedback on any measures taken, cf. the Directive relating to Oversight of the Intelligence, Surveillance and Security Services Section 7 final paragraph.'

In this case too, PST has referred to technical challenges relating to compliance with the regulatory requirements for

17 A script is a computer program that is designed to e.g. automatically identify registrations that are due for a manual review under the five-year rule.

18 The Police Register Act Sections 50 and 51, cf. the Police Register Regulations Section 25-2.

review of information, but stated that the service will look into possibilities for changing its practice. The Committee expects the matter pointed out to be remedied shortly, and will follow up the matter in 2017.

4.5 PST's processing of information about deceased persons

It follows from the Police Register Regulations Section 22-3 first paragraph that information should not be stored for longer than required to fulfil the purpose of the processing. PST has previously informed the Committee that if a person registered in Smart dies, the information about the person in question shall be deleted from Smart or extraordinary grounds be given for why it is necessary to continue to process information about him/her. In 2016, the Committee has noted that the service continued to process information in Smart about three persons after their deaths, and questioned the basis for this processing. As a result of the Committee's questions, PST deleted the information about these persons from the register.

The Committee criticised the service for having processed data about the persons for several years after their death without this being necessary.

The Committee noted that information about a total of 367 persons was processed in Smart after their death.

In the annual report for 2012, the Committee wrote that PST was considering whether to introduce a procedure that registers deaths, so that the information about deceased persons can be subjected to extraordinary review. When asked by the Committee in 2016, PST answered that no such procedure had been established.

The Committee stated to PST that the service should introduce such a procedure. At the same time, the Committee requested that PST should consider whether there are still grounds for processing information about all the persons who have died since their registration. PST stated that it is a weakness of this system that the registration of a death does not automatically trigger a request for review of the registration. The service stated that it is working on a monthly quality assurance and maintenance procedure for data registered in Smart that will include reviewing persons who have died. At the turn of the year, PST had not completed the review requested by the Committee.

The Committee notes that the service is working on a technical solution to ensure that registrations are reviewed shortly after the service receives information about the death of a registered person. In 2017, the Committee will follow up the service's review of information about persons who have died since their registration.

4.6 Oversight of PST's human intelligence source handling

On 13 March 2014, the Committee submitted a special report to the Storting concerning its investigation of allegations of politically motivated surveillance and PST's use of Christian Høibø as a human source. With reference to the special report and the Standing Committee on Scrutiny and Constitutional Affairs' remarks to the report,[19] the Committee decided to carry out spot checks in the service's human intelligence source handling system (KildeSys)[20]. In 2015, the Committee reviewed random samples from KildeSys that had been anonymised by PST. In 2016, the Committee expressed an expectation for PST to separate the identity of sources from KildeSys so that the Committee can conduct searches on its own in the system. The Committee's right of inspection of the service's handling of sources was a topic in the communication between the Committee and PST in 2016.

In the Committee's opinion, both the lessons learnt from the Committee's special report in 2014 and the above-mentioned spot checks in 2015 show that there is a need to oversee the information processed as part of PST's handling of sources. A key purpose is to 'to ascertain and prevent any exercise of injustice against any person', including the source him/herself, cf. the Oversight Act Section 2 first paragraph (1).

Pursuant to the Oversight Act Section 4, the Committee may 'demand access to the administration's archives and registers, premises, and installations of all kinds'. 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 PST, cf. the Directive relating to Oversight of the Intelligence, Surveillance and Security Service Section 6. The service is entitled to have any objections against such decisions recorded in the minutes and included in the Committee's annual report, cf. the Directive relating to Oversight of the Intelligence, Surveillance and Security Service Section 6. This will allow the Storting to conclude as to whether the Committee has sought more extensive access than necessary and thus correct the EOS Committee's line.

According to the Directive relating to Oversight of the Intelligence, Surveillance and Security Service Section 5 the Committee shall not seek more extensive access to classified information than warranted by its oversight purposes and observe the concern for protection of human sources. The EOS services cannot invoke this provision as a legal basis for denying the Committee access to information. Some of the Committee's search work in the services' systems involves refraining from further access as soon as it has been ascertained that no further access is warranted by the oversight purposes. The Committee and the Secretariat are very much aware of this part of the Storting's directive.

Written and verbal dialogue between PST and the Committee has shown that, although the parties do understand each other's points of view, PST has objections on grounds of principle against the EOS Committee's view that only a source's name and national identity number should be exempt from the Committee's regular oversight.

PST's objections are described in the Evaluation Committee's report:[21]

> 'PST's grounds for wanting to withhold information that could reveal the identity of a source from the EOS Committee's oversight at a general level is related to the risk that sources may stop sharing information with the service if it cannot guarantee its sources unconditional anonymity. In some cases, there could also be reason to fear for the life and safety of sources if this information was to become known.
> (…)
> Even though the name of the source is not included, PST refers to the fact that re-identification will always be possible because the information describes other identifying elements. PST's argumentation is not based on a concrete assumption that the EOS Committee will not observe its duty of secrecy, but on a general concern that there is an increased risk of information being spread if the EOS Committee is granted access.'

PST is also of the opinion that information other than the name of the source that can, seen together, lead to the source being identified (context information) must be exempt from the Committee's oversight.

What context information could result in a source being identified must be determined through discretionary assessment. If such an assessment is to be made by the service, the Committee could risk that PST will exempt more information than the Committee would consider warranted by the

19 Recommendation No 229 to the Storting (2013–2014).

20 The Committee described its follow-up of the special report in the annual report for 2014.

21 Document 16 (2015–2016) Report to the Storting from the Evaluation Committee for the Norwegian Parliamentary Intelligence Oversight Committee (EOS Committee), Chapter 42.

oversight purpose. This could interfere with the Committee's opportunity to achieve the purpose of the oversight. In order to be able to carry out the oversight function assigned to it by the Oversight Act, the Committee is of the opinion that it needs to be able to conduct its own searches in the systems where PST processes source material – but such that the names and personal identity numbers of the sources are not exposed.

The Directive relating to Oversight of the Intelligence, Surveillance and Security Service Section 13 subsection 3 letter g) states that the annual report should include 'a statement concerning any cases or matters which should be put before the Storting'. Based on the above, the Committee awaits the Storting's view on the Committee's future oversight of PST's source work in light of the account provided above.

4.7 New findings in a folder structure of PST's network

In the four previous annual reports, the Committee has criticised PST for processing intelligence information and personal data outside of the ordinary intelligence system. During an inspection in 2016, the Committee found further intelligence information on what is called the I area (in the Windows folder structure),[22] and the Committee asked PST to give an account of the processing of this information.

It is not a statutory requirement that intelligence information should be processed in specific systems, but the Act does stipulate requirements regarding specification of purpose, necessity and the relevance of the information. In order to comply with the quality requirements, PST has previously set out in its internal guidelines that intelligence information is only to be processed in the intelligence register Smart.

In its reply to the Committee, PST explained the service's needs to process intelligence information on the folder structure and that the above-mentioned internal guidelines will be amended because the current system 'does not promote the effective performance of the service's social responsibility. PST informed the Committee that the change will entail a need for internal control of the information stored on the file area.

The Committee took note of the fact that PST will change its guidelines and that work will be initiated to ensure that the service can also carry out internal control of the information processed in the file structure.

The Committee expects PST to also consider and facilitate the Committee's oversight of intelligence information during the announced work, and asked to be kept informed about the progress. Finally, the Committee requested a specific overview of all file areas that will be used to process intelligence information.

When concluding the case, the Committee remarked that, in light of the years of correspondence between PST and the Committee about the processing of information in the file structure, the Committee would have expected PST to inform it about this change in practice of its own accord.

4.8 PST's requests for registration of persons in the Schengen Information System (SIS)

The EOS Committee described PST's exchange of information though the Schengen Information System in its annual reports for 2014 and 2015. The Committee has been concerned with ensuring that the National Crime Investigation Service (Kripos) has sufficient information and underlying documentation to assess whether the conditions for SIS registration are met in cases where PST requests such registration. The Committee pointed out in its annual report for 2015 that the regulatory framework must be amended or clarified if special rules are to apply to PST's use of SIS.

The feedback provided by the Ministry of Justice and Public Security in April 2016 confirmed the Committee's understanding that PST must provide Kripos with the necessary underlying documentation to allow it to make an independent assessment of whether the conditions for SIS registration are met. If classified information is needed in order to assess whether the conditions for registration are met, but the PST is unwilling or unable to share such classified information with Kripos, then the person in question cannot be registered in SIS.

As regards the conditions for registration in SIS, the Ministry pointed out that there must 'be concrete indications that the person represents a serious threat to national security' and that 'the need for registration must (...) be based on objective facts indicating that the registration of information is required for the purpose of the registration'. In the Ministry's assessment, there is no basis for interpreting the term 'prevent' to entail a condition that 'grounds for suspicion' must exist, given that the other conditions stipulated in the provision are met.

The feedback from the Ministry of Justice and Public Security provided clarification in relation to the Committee's further oversight of PST on this point.

The continuous oversight of PST's requests for SIS registration in 2016 have left the Committee with the general impression that PST's requests for and prolongation of SIS registrations provide more comprehensive information to Kripos than before. The Committee has not asked PST questions about requests for SIS registration in 2016.

4.9 Information exchange with cooperating foreign services/agencies

4.9.1 Norwegian persons registered in the Terrorist Screening Center's (TSC) database

In its annual reports for 2013 and 2014, the Committee mentioned that it had been informed that information about quite a large number of Norwegians had been processed in a database belonging to the Terrorist Screening Center (TSC), an FBI unit tasked with identifying suspected or potential terrorists. The Committee has previously emphasised that it is problematic that information about Norwegian persons and persons with connections to Norway has been processed in the FBI database TSC without the basis for their registration being known. The annual report for 2014 described how the Minister of Justice and Public Security informed the Committee that he would continue to follow up the matter in relation to the American authorities and provide a satisfactory reply to the Committee's question once such clarification had been received.

In 2016, the EOS Committee asked the Ministry of Justice and Public Security for information about the status of the Ministry's follow-up of the matter since the Committee's annual report for 2014, including any further dialogue with the American authorities. The Committee has contacted the Ministry in connection with this matter on three separate occasions,[23] without receiving a reply.

During the Committee's inspection of the PST Headquarters in June 2016, PST stated that the service has raised the matter with the FBI. PST reportedly requested quality-assurance of the names in the database to ensure that persons who do not belong there are removed from the database.

4.9.2 Disclosing information to a foreign service

During one of the Committee's inspections in 2015, it reviewed intelligence information in Smart that showed that PST had received a request from a foreign service outside the EU to identify the owner of a phone number. The phone number had been used to make anonymous threats of explosions in a third country. PST sent the service in question information about a Norwegian citizen who owned the phone number, including personal data about the number of registered criminal cases and registrations in PO.[24]

Pursuant to the Police Act Section 17c, PST is charged with cooperating with other countries' police authorities and security and intelligence services, and the service can,

22 Windows Explorer can be used to view the folder structure of a hard disk/network station, including all files processed there, for example the I area (I:\).

23 The Committee's letters of 1 April 2016, 26 October 2016 and 12 January 2017.

24 The police operations log.

pursuant to the Police Register Act Section 22, disclose information to foreign parties in accordance with more detailed rules.

The Committee believed that the case should be followed up because it could be questioned whether it was necessary to disclose information about registered criminal cases and registrations in PO to the service in question. PST's reply to the Committee's question was that the service considered it necessary and relevant to inform the foreign service that the person in question was known to the Norwegian police. The reason for this was that it could not be ruled out that this person had called in the threats of explosions, even though PST had indications that the phone number might have been used by a third person. Information about the person would better enable the third country's service to assess the situation and deal with the threats. PST also considered it important to give the foreign service the best possible information in the case 'due to considerations of maintaining a satisfactory cooperation with the country in question's services in the counterterrorism field'.

Moreover, PST stated that up-to-date procedures now exist for disclosing information that, among other things, ensures that a special risk assessment is carried out when disclosing personal data to countries outside the EU. According to PST, the service ensures, to a greater extent than previously, that assessments made during the process are documented.

In its concluding letter to PST, the Committee pointed out that 'considerations of maintaining a satisfactory cooperation with [the country in question's] services in the counterterrorism field' does not appear to be relevant to the assessment of whether to disclose personal data about a Norwegian citizen to the foreign service. The Committee remarked that 'considerations of protection of [the person's] privacy must take precedence over the desire for satisfactory cooperation with the [country in question's] services'.

Otherwise, the Committee did not pursue the matter further after receiving the service's statement, since the Committee concluded that PST's response was satisfactory concerning the assessment of whether it was necessary and relevant to disclose information to the foreign service.

4.10 PST's assistance to the police

PST can assist the ordinary police both in criminal cases and other cases. The service's right to cooperate with and assist the ordinary police is expressly warranted in certain cases.[25] The Committee has previously stated to PST that it agrees that these provisions are not an obstacle to PST cooperating with the ordinary police if requested also in areas other than those expressly mentioned. It is stated in the PST Regulations Section 9 third paragraph that PST can assist the ordinary police in connection with 'combating organised crime and crimes against humanity, genocide and serious war crimes'.

4.10.1 Assistance to the police in a criminal case

In its annual report for 2014, the Committee stated that it had asked questions about an intelligence registration established as a result of a case where PST provided assistance to the ordinary police. PST was of the opinion that the raw material from such assignments can be stored for 'as long as is deemed necessary'.

With reference to the Police Register Section 21-1 (7), where it is stated that only information about what information has been disclosed, who the recipient was and why the information was disclosed can be processed, the Committee pointed out, among other things, that PST does not have legal authority to process raw data after completing the assistance task. The Committee remarked that the basis for processing information associated with cases in which PST provides assistance was unclear, and PST agreed with this assessment. PST intended to raise the ambiguity in the rules regarding processing of information associated with cases in which it assists the police with the Ministry of Justice and Public Security.

The Ministry later made the following statement concerning this issue:

> 'The Ministry agrees that the Police Register Act Section 64 third paragraph (5) does not warrant processing information in such cases, but does not see a need to amend the Police Register Act. When PST assists other police entities in investigations pursuant to the Police Act Section 17b second paragraph, this involves processing of information in criminal cases. Both Section 5 (1) and Section 64 second paragraph of the Police Register Act state that information in criminal cases is processed in accordance with the provisions of the Criminal Procedure Act, and that this applies until the criminal case has been finally concluded. Therefore, the Police Register Act contains no special provisions concerning the processing of information in criminal cases. Reference is also made to the fact that the Police Register Act was not intended to entail any changes in relation to previous law as regards the processing of information in criminal cases.
>
> In the Ministry's opinion, it will be natural for the information obtained by PST in connection with assistance provided to be included in the documents in the criminal case or registered as part of the internal case processing, cf. the Police Register Regulations Section 26-2.

> Once the criminal case has been concluded, PST cannot process the information further unless an independent basis exists for processing the information pursuant to Section 64 of the Police Register Act. To the extent that PST needs to document how assistance was provided after the criminal case has been concluded, the Ministry assumes that such information can be stored without including personal data.'

The Committee took note of the Ministry of Justice and Public Security's account, and noted that 'PST takes note of the Ministry's statement and will find a solution to implement its interpretation of the law shortly'. The Committee later took note of PST's accounts of this.

The Committee also noted that information processed about the person in question in the intelligence registrations in Smart would be deleted. On the basis of the information registered, the Committee also found grounds for pointing out that the scope of the Police Register Act is not limited to personal data. The Act also regulates PST's processing of information about legal persons, among other things, cf. the Police Register Act Section 3.

4.10.2 Assistance to the police outside criminal cases

PST did not give a direct answer to the Committee's other questions about the service's basis for processing information/personal data when assisting the ordinary police *outside criminal cases*. Considering the fact that PST stated that it has not provided such assistance involving processing of personal data to the ordinary police in the past ten years, the Committee let the matter rest after receiving PST's statement.

4.11 Complaint cases considered by the Committee

The Committee received 20 complaints against PST in 2016, compared with 14 complaints in 2015. The Committee's 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. The Directive relating to Oversight of the Intelligence, Surveillance and Security Service states that statements given in response to complaints against PST shall only state whether or not the complaint contained valid grounds for criticism.[26]

The Committee expressed criticism against PST in two complaint cases in 2016. In both cases, the Committee submitted a request to the Ministry of Justice and Public Security for more detailed feedback to be given, cf. the Directive relating to Oversight of the Intelligence, Surveillance and Security Services Section 8 second paragraph. The Ministry has yet to respond, despite postponed deadlines and several reminders. At the time of the Committee's final consideration[27] of this annual report, two and three months have passed, respectively, since the Committee's initial enquiries to the Ministry in these cases.[28] As a consequence, complainants experience unreasonably long case processing time for their complaints to the Committee. It is incomprehensible why the Ministry of Justice and Public Security has not responded to the Committee's requests.

The Committee's limited possibility to give complainants grounds for its criticism of PST in complaint cases continues to represent a great challenge for the Committee, see Chapter 3.

25 Cf. the Police Act Section 17b second paragraph and Section 17b third paragraph, cf. the PST Regulations Section 9 third paragraph and Sections 5 and 6.

26 Cf. the Directive relating to Oversight of the Intelligence, Surveillance and Security Services Section 8 second paragraph: 'Statements to complainants should be as complete as possible without revealing classified information. Statements in response to complaints against the Police Security Service concerning surveillance activities shall however only state whether or not the complaint contained valid grounds for criticism. If the Committee holds the view that a complainant should be given a more detailed explanation, it shall propose this to the Ministry concerned.'

27 The Committee's final consideration of the annual report for 2016 took place in a meeting on 15 February 2017.

28 The Committee contacted the Ministry of Justice and Public Security on 14 November 2016 concerning one of the complaint cases and on 20 December 2016 in connection with the other case.

5.
The National Security Authority (NSM)

5.1 General information about the oversight

The Committee carried out four inspections of NSM in 2016, including one of NSM NorCERT.[29]

During its inspections of the directorate, the Committee focuses on the following:

- NSM's processing of cases where security clearance has been denied, reduced or suspended by the security clearance authority, and its processing of complaints in such cases
- NSM's cooperation with other EOS services

During the inspections, the Committee is regularly briefed about NSM's ongoing activities, including its cooperation cases with other EOS services and case processing time in security clearance cases.

5.2 Case processing procedures in security clearance cases

Security clearance cases start with the person for whom security clearance is sought filling in information about him/herself and his/her closely related persons in the personal particulars form. The employer (requesting authority) submits the form, along with a request for security clearance, to the security clearance authority. The security clearance authority obtains information about the person in question from a number of registers and carries out an assessment, based on the information provided by the person him/herself and obtained from the register, of whether the person concerned is fit to process sensitive information. If the requested security clearance is granted, the employer will be notified. If the requested security clearance is not granted, the person concerned will be notified and given grounds for the decision and the opportunity to appeal the decision.

The Public Administration Act Section 11a stipulates a requirement for cases to be prepared and decided without undue delay. If it is not possible to answer an enquiry in a case concerning an individual decision within one month of receiving it, a provisional reply shall be given containing information about when a reply can be expected and why the enquiry cannot be dealt with earlier.

The Committee has noted several cases involving appeals against negative security clearance decisions in which it took a long time for the cases to be decided and the person concerned either did not receive information from NSM about the expected case processing time or it took several months for such information to be sent.

In connection with an inspection of NSM, the Committee asked about its procedures for sending such provisional replies. NSM stated that, as a result of the Committee's questions, it established new procedures and tightened the existing procedures in order to meet the Public Administration Act's requirements concerning the duty to provide guidance and provisional replies.

The Committee notes that NSM has established procedures to ensure that the persons concerned are informed about the progress in their cases. In periods of very long case processing time, as has been the case for NSM, it is very important to the persons in question to be informed about when they can expect their case to be decided.

In the Committee's annual report for 2013,[30] it requested that NSM review its procedures for handling access to documents. During 2016, the Committee requested feedback from NSM about this work. In its reply, NSM stated that the work on a guide to access work has been given lower priority for capacity reasons, but that the work has been resumed and that the directorate aims to publish the guide in 2017.

In its concluding letter to NSM, the Committee pointed out that a long time has passed without the guide being put in place, and urged NSM to make work on this guide a priority in 2017. The Committee shares NSM's expectation that the guide will have a significant effect in terms of equal treatment, efficiency and security in connection with requests for access.

5.3 Case processing time in security clearance cases

In its five last annual reports, the Committee has pointed out that case processing time are far too long in many security clearance cases. In its annual report for 2015, the Committee found that NSM had implemented measures that had reduced the backlog and gave reason to expect the case processing time of more recently received cases to be shorter. The Committee noted that security clearance cases were still not decided quickly enough, and expected NSM to continue its efforts to bring case processing time in security clearance cases down to a satisfactory level in 2016.

29 NSM NorCERT (Norwegian Computer Emergency Response Team) is Norway's national centre for coordination of incident management in connection with serious ICT security incidents. NSM NorCERT is a function attended to by NSM's Department for ICT Security.

30 See Chapter V section 7 in the Committee's annual report for 2013.

The basis for the Committee's focus on case processing time in security clearance cases is that a decision in a security clearance case is often of vital importance to a person's life situation and future career. During its inspections of NSM in 2016, the Committee has requested information about case processing time in security clearance cases. The measures implemented have resulted in a reduction in average case processing time for requests for security clearance and appeals against negative security clearance decisions. In connection with the Committee's inspection in December 2016, NSM stated that the average case processing time for appeals against security clearance decision as an appeal body was 82 days. At the time of the inspection in March 2016, the corresponding case processing time was 319.5 days.

The Committee notes that the average case processing time for security clearance cases has been significantly reduced in 2016. However, the situation remains unsatisfactory for all individuals whose security clearance cases take considerably longer than average to process. It is important that NSM continues to focus on case processing time in security clearance cases.

In 2016, the Committee has also been briefed about case processing time in cases concerning requests for access to information in security clearance cases. In March 2016, the average case processing time for requests for access was just over seven months. In December 2016, the average case processing time was just under two months. Since requests for access rarely involve material questions of doubt, this case processing time is in any case too long.

The Committee has raised questions relating to case processing time for requests for access with NSM. The Committee stated that the very long case processing time in individual cases concerning access warrants criticism, particularly with reference to the fact that appeals against security clearance decisions shall not be processed (and need not be submitted) until the request for access and, if relevant, appeal against a decision to deny access, have been processed. Combined, this could result in it taking an extremely long time for the person concerned to receive clarification on the matter.

The Committee notes that the average case processing time for requests for access has been significantly reduced in 2016. In the Committee's opinion, the case processing time should still be considerably reduced. The Committee expects NSM to continue to give priority to this area.

5.4 NSM's security interviews

The Committee stated in its annual report for 2015[32] that, based on its 2015 review of how security interviews were conducted, it would carry out oversight activities in relation to more security interviews conducted by NSM in the course of 2016. The Committee was of the opinion that NSM took the problems associated with security interviews that the Committee had pointed out seriously, and was satisfied that NSM would implement more measures in this area in the time ahead. Based on the 2015 review of security interviews, the Committee concluded that it would not be necessary to implement an external evaluation of how security interviews are conducted.

Table of case processing time given in connection with inspections:

	Inspection, March		Inspection, September		Inspection, December	
Types of cases	Number	Average case processing time	Number	Average case processing time	Number	Average case processing time
Requests for access	5	230 days	15	127 days	6	59 days
Requests for security clearance	425	131	511	98	187	89
First-tier appeals	7	396	5	177	8	214[31]
Second-tier appeals	53	320	35	104	29	82

In 2016, the Committee continued its work to review and carry out oversight activities in relation to security interviews conducted by NSM, including by having the whole Committee review recordings of some interviews. The Committee's interest in how security interviews are conducted are based on considerations of due process protection and equal treatment in particular.

During an inspection of NSM in 2016, the Committee selected two security interviews for thorough review (by reviewing audio and video recordings). Before the inspection, the two interviews in question were identified to NSM, which reviewed them beforehand. During the inspection, NSM gave an account of its work to improve the way in which security interviews are conducted and provided information about concrete measures implemented since the Committee's inspection in November 2015, where security interviews were also a core topic. NSM was also asked to comment on the way in which the two security interviews were conducted.

On the basis of the review, NSM stated that some of its main findings related to weaknesses in preparations for the interviews and interviewers' poor ability to make use of information provided by the interviewee during the interview. NSM could not see any clear non-conformities in terms of interview technique or the suitability of questions, the use of closed questions or breaks.

During the meeting, the Committee asked questions and provided input to NSM. The Committee remarked that in one case, it took the interviewer far too long to get to the core topic, and the interview was far too detailed – without the purpose of the interview being fulfilled. *In recent years, the Committee has reviewed a number of security interviews. Aspects of these conversations raise doubts about whether the way in which NSM conducts security interviews contributes to shedding light on the assessment criteria sound judgement, reliability and loyalty and thus helps to elucidate the case.*

The Committee also noted that the interviewees were filmed during breaks in the security interviews when the interviewers had left the room, without being informed of this before the interview. In the Committee's opinion, this entails a significant violation of integrity. *The management of NSM immediately decided to discontinue video recording of interviewees during breaks with immediate effect. The Committee is satisfied with this.*

The Committee expresses a positive view of the fact that NSM continues its work to improve the way in which security interviews are conducted, and notes that it has taken steps towards achieving this.

The Committee has also been informed that NSM sent a project application concerning development of security interviews to the Ministry of Defence.

The Committee will continue its dialogue with NSM on how security interviews are conducted and follow the improvement work closely in its oversight of the way in which NSM conducts security interviews.

5.5 Conditional security clearance etc.

In 'special cases', security clearance can be granted subject to conditions, cf. the Security Act Section 21 fifth paragraph. According to the preparatory works to the Act,[33] conditions are primarily intended to be used in situations where a person has a connection to another country and there is a hypothetical risk that this connection could, in a given situation, form the basis for a high security risk.

In connection with its inspections of NSM in 2015, the Committee asked to be sent a security clearance case in which the internal grounds[34] for the security clearance decision showed that the person concerned was granted the requested security clearance 'on the condition that he notifies [the department's security officer] if his contact with his family becomes more frequent, if he is asked to support relatives or other persons financially, or if he is contacted by the authorities of another country'. NSM communicated this information in a letter to the person responsible for authorisation,[35] and stated that the person concerned should report it if any of the above-mentioned situations arose.

The Committee asked NSM to clarify whether or not a conditional security clearance had been granted in this case. If conditions were set for granting clearance, NSM was asked to give an account of whether the statutory requirement for 'special cases' had been met. The Committee also pointed out that a special duty to provide information appeared to be imposed on the person in question, and asked NSM to explain whether such a duty could be considered anything other than a condition.

31 One case with a processing time of 760 days increased the average significantly.

32 The EOS Committee's annual report for 2015, section 5.4.

33 Proposition No 59 to the Odelsting (2004–2005), page 10.

34 Cf. the Security Act Section 25 last paragraph.

35 Cf. the Security Act Section 20 sixth paragraph.

NSM stated in its reply that the word 'condition' had been used inadvertently and that no conditions were attached to the security clearance. It also stated that it was not common practice at NSM to impose special duties on personnel who have been granted security clearance as part of the communication of vetting information to the person responsible for authorisation. NSM considered the above-mentioned matters to be covered by the person in question's general duty to provide information, but specified them in more detail in its contact with the person responsible for authorisation. Failure on the part of the person concerned to report such matters could potentially have a bearing on his security clearance.[36]

When concluding the case, the Committee described it as unfortunate that the wording of the conclusion in the internal grounds did not reflect the outcome of the case.

The Committee also referred to the fact that the general duty to provide information is deemed to apply to matters as described in the Security Act Section 21 first paragraph letters a–j, in practice any changes to the matters that the person concerned has described in the personal particulars form.[37, 38] It is not stated in the personal particulars form or the guide to completing this form that personnel who have been granted security clearance should report the frequency of contact with their family (in their home country). If a duty to report changes in the frequency of contact with his family on a continuous basis was to be imposed on the person concerned, this duty would, in the Committee's opinion, have to be based on a special duty to provide information.

The Committee emphasised that failure to provide information about matters that the personal particulars form does not contain questions about in contexts other than when asked a direct question by the person responsible for authorisation can hardly be deemed to constitute a breach of the person in question's general duty to provide information.

5.6 Advance notification of a security clearance decision

The Committee has considered a case in which NSM as the initial security clearance authority gave advance notification of a negative decision to the requesting authority. The consequence was that the person concerned was removed from the top of the recommendation list for the position for which security clearance had been sought. In this case, NSM informed the requesting authority that the person in question would not be granted the requested security clearance before a decision had been reached in the security clearance case.

After having given advance notification of its decision, NSM was informed by the requesting authority that the name of the person in question was removed from the recommendation list. Instead of providing guidance to the requesting authority that, regardless of the decision reached in the first instance, the person concerned would be entitled pursuant to the Security Act to have the case considered by the appellate body (the Ministry of Defence), NSM closed the case. NSM reopened the security clearance case following a request from the person concerned, and the case was later forwarded to the appellate body for consideration. The appellate body reversed NSM's negative decision and granted the requested security clearance. This means that the person in question could have taken up the position he had applied for, had it not been for this error on the part of NSM.

NSM also denied the person in question access to the correspondence between NSM and the requesting authority

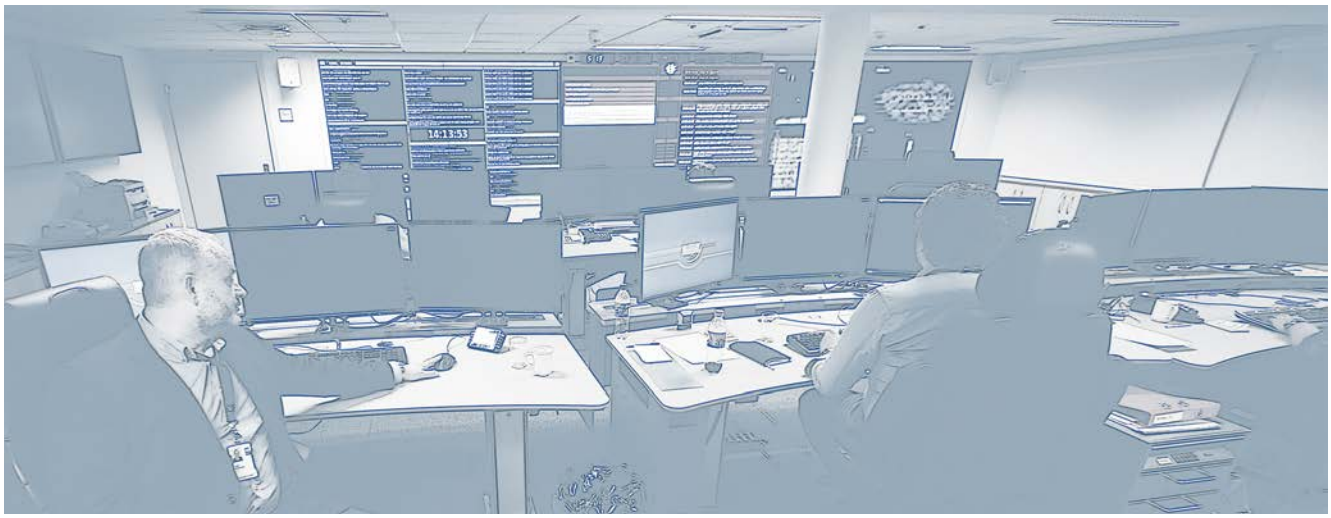


Photo: Olav Olsen / Aftenposten / NTB scanpix

without having a legal basis for denying access to these documents in the case. NSM has informed the Committee that the person in question will now be granted access to the documents.

NSM has acknowledged the errors pointed out by the Committee.

In its concluding statement to NSM, the Committee stated the following:

> 'In the Committee's opinion, the errors committed warrant strong criticism and constitute a clear injustice to the citizen. [The person's] due process protection was violated, and this had serious actual consequences in that he lost the top place on the recommendation list.'

5.7 Project concerning security clearance of persons with connections to another state

In its oversight of security clearance cases, the Committee has over several years identified matters of principle in cases where the person concerned or his/her closely related persons have connections to other states, especially states with which Norway has no security cooperation. If no such security cooperation exists, information with a bearing on the assessment of the person in question's suitability for security clearance cannot be obtained in connection with vetting.

Connections to another state exists e.g. when the persons concerned or their closely related persons are citizens of another country or have close family ties, property or financial interests or contact with the authorities in the foreign state. Any form of connection to a foreign state is not in itself sufficient grounds for denying security clearance, and the degree of connection must be taken into consideration as part of an overall assessment.

In 2016, the Committee decided to conduct a systematic review of a large number of cases where persons for whom security clearance had been requested or their closely related persons have connections to another state. The purpose of this project is to uncover any unwarranted differences in how the security clearance authorities deal with similar cases and to determine whether the case processing complies with the statutory requirements. The Committee expects to complete this project in 2017.

5.8 Complaint cases considered by the Committeet

5.8.1 Introduction

The Committee received six complaints against NSM in 2016. The complaints concerned security clearance cases. Due to the complexity and scope of these complaint cases, the Committee has used a great deal of resources on them. A decision in a security clearance case is often of vital importance to a person's life situation and future career. It is therefore essential that these cases are considered by the security clearance authorities in a fair manner that safeguards due process protection. In cases where the Committee express criticism, the grounds for the Committee's decision are regularly communicated to the complainant.

Of the cases that the Committee concluded in 2016, the following three cases gave grounds for critical remarks from the Committee:

5.8.2 Complaint case 1 – invalid decision by NSM

In an appeal to the Committee against NSM's decision to uphold a decision to deny security clearance, the Committee asked NSM several questions about the security clearance authority's assessment of the person concerned's use of intoxicants, in addition to questions about the elucidation of the case, case processing time and the grounds for the decision.

NSM based its decision on the person in question having provided incorrect information in the personal particulars form about his use of illegal intoxicants, cf. the Security Act Section 21 first paragraph letter d, since he had used cannabis abroad in the past ten years.

The Committee remarked that it can be claimed that the information that the person in question provided in the form could have been more satisfactory, but points out that the important issue for the security clearance authority must be that the person did provide information about his use of cannabis. The security clearance authority would not have known about the person's cannabis use had he not provided this information himself, and the Committee therefore found it unreasonable to conclude that the person in question had misrepresented the facts to the security clearance authority.

NSM had made reference to the fact that it was illegal for tourists to use cannabis in the other country. Among other things, the Committee pointed out that it is the outlet in

36 Cf. the Security Act Section 21 first paragraph letters d) and g).

37 It is stated in the introduction to the personal particulars form that: 'If there are any changes in relation to the information you have stated on the form, it is your duty to inform your authorising authority.'

38 NSM's guide to the Security Act Chapter 6 and the Regulations concerning Personnel Security page 18.

question that is in breach of the regulatory framework if it sells cannabis to a tourist, not the tourist him/herself. NSM had thus based its decision in the person in question's security clearance case on an incorrect interpretation of the other country's criminal law.

With reference to the fact that the person in question's use of cannabis abroad was *legal under Norwegian criminal law*, the Committee found that he had answered the question in the personal particulars form correctly. There is thus no basis for NSM's claim that he tried to mislead the security clearance authority.

In NSM's view, the person in question's grounds for no longer using cannabis in Norway gave rise to considerable doubts about his suitability for security clearance, including about whether he would comply with the applicable legislation in this area. The Committee found it difficult to see how it could be considered a negative factor that a person who may support the legalisation of cannabis states that his decision to not use cannabis is based on a wish not to support criminal groups. On the contrary, this decision seems to indicate that the person in question has been loyal to the current legislation, even though he might wish it amended.

Security clearance decisions should be based on a specific and individual overall assessment, and the security clearance authority shall seek to clarify unclear matters, cf. the Security Act Section 21 third paragraph.

The Committee remarked that NSM had not mentioned a single factor that benefitted the person concerned, not even the statement from his employer. This left doubt as to whether NSM had considered factors that benefitted the person in question. The Committee criticised NSM for not having done enough to elucidate the case, including by holding a new security interview during the complaint review.

The Committee also criticised NSM for having taken more than one year and two months to give the person concerned access to the documents in the case. In light of how crucial the right of access is to the person's possibility to safeguard his own interests, the Committee is of the opinion that NSM's failure to follow up the request for access constituted a breach of good administrative practice.

NSM was also criticised for the long case processing time in the complaint case. It took NSM ten months to consider the complaint, even though NSM found the case to have been sufficiently elucidated during its initial consideration. The Committee stated that the case processing time in the complaint case did not meet the requirement stipulated in the Public Administration Act Section 11a first paragraph, which stipulates that cases should be decided 'without undue delay'.

Based on the Committee questioning whether the grounds given to the complainant met the requirements stipulated in the Security Act Section 25 third paragraph, NSM sent the person concerned a letter where it referred to the grounds provided by the authority that made the initial decision. The Committee pointed out in its concluding statement that this did not give the person in question more detailed grounds for the decision, since it did not describe the factors on which the security clearance authority had placed decisive weight. The Committee stated:

> 'In the Committee's opinion, a decision to deny security clearance is so invasive that it strengthens the requirement that the grounds given must be sufficiently precisely and clearly worded, so that they reflect the considerations that have been decisive in the case. The lack of grounds has made it difficult for [the person in question] to respond to the decision and weakened his due process protection. In a case such as this one that focuses so much on the attitudes of the person in question, it is important that the security clearance authority provides as satisfactory grounds as possible.
>
> It is the Committee's opinion that [the person in question] has not received grounds that meet the requirements of the Security Act Section 25 third paragraph. NSM is to blame for this.'

Finally, the Committee stated that it had found several instances of errors and negligence in NSM's case processing, and that on this basis it found that an injustice had been committed against the person concerned, cf. the Oversight Act Section 2(1). In the Committee's opinion, the errors committed and negligence shown by NSM was of such a nature that the decision to deny the person concerned security clearance was invalid, cf. Directive relating to Oversight of the Intelligence, Surveillance and Security Service Section 7 second paragraph, which refers to the Act concerning the Storting's Ombudsman for Public Administration Section 10 second paragraph.[39]

The Committee urged NSM to carry out a new and unbiased assessment of the case, cf. the Directive relating to Oversight of the Intelligence, Surveillance and Security Service Section 7 final paragraph.

NSM reconsidered the complaint case. Following a new specific and individual overall assessment, NSM granted the appeal and the person in question was granted the requested security clearance. ***The Committee is satisfied that NSM has reconsidered the case.***

5.8.3 Complaint case 2 – long case processing time in security clearance and access case

In 2016, the Committee received a complaint against NSM and FSA[40] concerning long case processing time in a security clearance and access case.

After the FSA forwarded the appeal to NSM, it took NSM 457 days to uphold FSA's initial decision. NSM's case processing time in the access case was approximately one year and two months from all the documents in the case had been forwarded until a decision was made in the access case.[41] Even though it was taken into account that circumstances on the part of the complainant had a bearing on the case processing time in the complaint and access cases, the Committee expressed the opinion that the case processing time was in any case unreasonably long.

Among other things, the Committee stated the following in its concluding letter to NSM, of which the complainant was also informed:

> 'In the Committee's opinion, the case processing time in the access cases and security clearance cases both in the FSA and NSM were far too long. A total case processing time of 1,047 days from [the person in question] appealed the FSA's decision in the security clearance case on 29 April 2013 until NSM as the appellate body made its decision on 11 March 2016 warrants strong criticism regardless of the facts of the case. The Committee finds reason to criticise FSA and NSM for unreasonably long case processing time in the consideration of [the person in question's] security clearance case.'

The Committee expects to find no security clearance cases with anywhere near as long case processing time in future.

5.8.4 Complaint case 3 – access and grounds

On the basis of a complaint, the Committee criticised NSM for having taken five months to consider a request for access. The Committee also criticised the fact that the negative security clearance decision was made before all the documents in the case had been completed. The Committee found it difficult to understand that the minutes of the security interview did not appear to have been completed until five months after the decision was made. At the time the decision to grant access was finally made, NSM had still not completed the minutes of the security interview.

NSM was also asked to consider giving the complainant somewhat more detailed grounds for the decision to deny security clearance, better highlighting which factors NSM did and did not emphasise, compared with the body that made the initial decision's consideration of the case. The basis for this was particularly that the information provided to the complainant by NSM did not show that NSM and the body that made the initial decision attached different importance to criminal offences.

Initially, NSM was of the opinion that the complainant had received satisfactory grounds during the complaint case. The Committee disagreed and requested that NSM consider again whether to give the complainant somewhat more detailed grounds for the decision to deny security clearance. NSM then provided new grounds to the complainant which the Committee also found to be unsatisfactory. The Committee pointed out that it was regrettable that the complainant was still not informed about the difference in importance attached to criminal offences by the body that made the initial decision and NSM, a factor which was important to the complainant. The Committee attempted to clarify these circumstances in its concluding letter to the complainant.

39 The Committee shall base its oversight and the formulation of its statements on the principles set out in Section 10 first paragraph and Section 10 second paragraph, first, third and fourth sentences of the Act concerning the Storting's Ombudsman for Public Administration. This provision states that the Ombudsman may call attention to errors that have been committed or negligence that has been shown in the public administration. The Ombudsman may also, if he concludes that a decision must be considered invalid or clearly unreasonable or that it clearly conflicts with good administrative practice, express this opinion.

40 See section 6.3.2.

41 See section 5.3.

6.
The Norwegian Defence Security Department (FSA)

Photo: Forsvaret

6.1 General information about the oversight

The Committee conducted three inspections of the FSA in 2016.

During its inspections of this department, the Committee focuses on the following:

- The FSA's processing of security clearance cases
- The FSA's cooperation with other EOS services
- The FSA's protective security activities

During the inspections, the Committee is regularly briefed about the FSA's ongoing activities.

The FSA's processing of security clearance cases is particularly important in the Committee's oversight of the department. The FSA is Norway's largest security clearance authority by far. The Committee reviews most of the negative security clearance decisions made by the FSA that have not been appealed, as well as appealed security clearance cases where the department granted the appeal in part or in full.

The Committee also oversees the FSA's protective security activities, and, in that connection, carries out spot checks of investigations into activity that poses a threat to security targeting the Armed Forces (security investigations) and operational cases that are part of the FSA's responsibility for military counterintelligence (Mil CI) in Norway in peacetime. One of the Committee's primary duties in this connection is to oversee the FSA's processing of personal data as part of its protective security activities.

In 2016, the FSA has facilitated the Committee's searches in the department's systems, including by providing guidance on how to conduct searches.

The Committee received four enquiries and complaints against the FSA in 2016. One of the complaints resulted in criticism from the Committee against the FSA for long case processing time in a security clearance case, see section 6.3.2.

6.2 Processing of personal data by the FSA

6.2.1 Introduction

The Committee regularly oversees the FSA's processing of personal data. This topic has been referred to e.g. in the annual reports for 2010,[42] 2011,[43] 2012,[44] and 2015.[45]

Since the reference in 2015, the Committee has asked to be kept informed about the ongoing work relating to the regulatory framework for processing of personal data in the FSA. On 17 August 2016, the head of the FSA adopted the Provisions relating to the processing of personal data in defence security service. The FSA has stated that these provisions are expected to be approved by the Ministry of Defence and should be ready for implementation in spring 2017. The provisions will apply to all units in the Armed Forces, except for the Norwegian Intelligence Service. The purpose of these provisions is 'to establish an internal control system for the performance of security service activities that will, among other things, ensure the quality of information and safeguard due process protection and protection of privacy'. The provisions are useful to the Committee's oversight of the FSA's processing of personal data, among other things. It remains to be seen what practical effect they will have on the processing of information as part of the performance of security service in the Armed Forces.

6.2.2 Processing of information about journalists

In 2016, the Committee concluded two cases concerning FSA's processing of information about journalists in the FSA's network.

6.2.2.1 Processing of information about several journalists in connection with the investigation of a security breach

In connection with the investigation of a serious security breach (an incident that poses a threat to security), the FSA processed the names of several journalists in an overview of the case. The Committee raised the matter of this processing with the FSA, even though the information had subsequently been deleted. The FSA stated that the names were included because the journalists were 'potential recipients' of classified information from the security breach. The FSA referred to the fact that the journalists' names were part of the investigation of the incident that posed a threat to security, but that no further investigative steps were taken in relation to these people.

In its concluding letter to the FSA, the Committee pointed out that it could not see any assessments of the necessity

42 Chapter V section 3.
43 Chapter VI section 4.
44 Chapter VI section 6.
45 Chapter 6 section 6.3.

or relevance of processing information about the journalists in the overview of the case. The Committee emphasised that, generally speaking, it is a serious matter if the EOS services process information about people as a result of their activity as journalists without sufficient grounds.

6.2.2.2 Processing of information about one journalist

During an inspection of the FSA in 2015, the Committee observed that the department was processing information about a journalist, including a report that contained information from open sources about the date of birth, home address, tax information, information registered in the Brønnøysund Register Centre and media articles about the Armed Forces over an extended period of time.

In its concluding letter, the Committee referred to the fact that the FSA can only process information that is required for the purpose of the performance of the FSA's duties, cf. the Personal Data Act Sections 8 and 11 and Instructions for Defence Security Service Section 19.

The Committee criticised the FSA for having processed the information about the journalist without legal authority and in violation of the Personal Data Act. In the Committee's opinion, it is unfortunate that personal data about a journalist and his journalistic activities were collected and stored for about four years without sufficient legal basis for this processing.

The Committee noted that the FSA already before its inspection acknowledged that it had made a mistake and expressed that the department would take steps to delete the documents after the inspection. The FSA stated that this processing was the result of a case processing error.

The Committee referred to a similar case referred to in the annual reports for 2012 and 2013, in which the Committee criticised the Intelligence Battalion (Ebn) for having processed corresponding information about journalists without sufficient legal basis.[46]

The Committee emphasised in its communication with the FSA that the press attends to important tasks such as information, debate and social criticism and enjoys strong protection through e.g. freedom of expression and freedom of the press. The Committee expects not to find such information with the FSA again.

Photo: Forsvaret

6.2.3 Processing of personal data in the records of the military counterintelligence section

The Committee noted during an inspection of the FSA that the department processed information about several persons in the records of the military counterintelligence section. The Committee questioned whether it is expedient to process personal data in these records, and how the FSA ensured that the information was correct and up to date and was not processed for longer than required. The Committee asked the department to explain the legal basis[47] for processing information about specific persons, including whether there was a basis for continuing to processing the information.

The FSA stated that the department has no system for ensuring that personal information in the records are not processed for longer than required for the purpose of the processing and that the personal data are correct and up to date. The FSA acknowledged that the present arrangement is problematic and hoped that the situation would improve shortly when the section introduces a new information system. As a result of the Committee's questions, the FSA deleted the information about twelve persons from the records.

In its concluding statement in 2016, the Committee criticised the FSA for having stored personal data about the twelve persons in question for longer than required for the purpose of the processing. The Committee stated that the FSA should introduce a system to ensure better compliance with the regulatory requirements regarding the quality of information. In the subsequent correspondence, the FSA has taken note of this criticism and stated that new procedures have been put in place.

6.3 Complaint cases considered by the Committee

6.3.1 Introduction

The Committee received four complaints and enquiries against the FSA in 2016. Due to the complexity and scope of some of these cases, the Committee has used considerable resources on them. A decision in a security clearance case is often of vital importance to a person's life situation and future career. It is therefore essential that these cases are considered by the security clearance authorities in a fair manner that safeguards due process protection.

In cases resulting in criticism, the complainant can also in many cases be informed of the grounds for the Committee's conclusion.

Of the cases the Committee concluded in 2015, the following case gave grounds for critical remarks from the Committee:

6.3.2 Complaint case – long case processing time in security clearance and access case

In 2016, the Committee received one complaint against the FSA and NSM concerning long case processing time in a security clearance and access case that resulted in criticism of the security clearance authority. See the description of this case in section 5.8.3.

After an appeal against the FSA's security clearance decision was filed, it took the FSA 590 days to uphold its own decision in the initial consideration of the appeal and make a decision in the access case.

The Committee noted that the FSA wrote that this is a long case processing time under any circumstances and apologised for this. The FSA stated that this is not a normal case processing time for its appeal cases. In its reply to the Committee, the department cited as factors that had affected the case processing time a large backlog, problems with the audio recording of the security interview, circumstances relating to the complainant and problems relating to the introduction of a new case processing tool in 2014.

The Committee stated the following in its concluding letter to the FSA, of which the complainant was informed:

> 'In the Committee's opinion, the case processing time in the access case and security clearance case in the FSA were unreasonably long. A total case processing time of 590 days from [the person in question] appealed the FSA's decision in the security clearance case on 29 April 2013 until the FSA upheld its own decision in the security clearance case and in the access case on 10 December 2014 warrants strong criticism regardless of the facts of the case. The Committee finds reason to criticise the FSA for the unreasonably long case processing time in the consideration of [the person in question's] security clearance case.'

The Committee expects to find no cases with anywhere near as long case processing time in the FSA in future.

46 Document 7:1 (2012–2013) Annual Report to the Storting from the Norwegian Parliamentary Intelligence Oversight Committee (EOS Committee) for 2012, part VIII section 4 page 34, and Document 7:3 (2013–2014) Annual Report to the Storting from the Norwegian Parliamentary Intelligence Oversight Committee (EOS Committee) for 2014, part VIII section 4 page 36.

47 These legal requirements follow from the Personal Data Act Section 11 first paragraph letter e and Section 28, as well as from the Instructions for Defence Security Service Section 20 first paragraph letter c.

7.
The Norwegian Intelligence Service (NIS)

7.1 General information about the oversight

The Committee conducted four inspections of the NIS headquarters in 2016, in addition to one inspection of the NIS unit at the Norwegian Armed Forces' Joint Headquarters (NJHQ), see section 8.1.

The Committee shall ensure that NIS's activities are carried out within the framework of the service's established responsibilities, and that no injustice is done to any person, cf. the Directive relating to Oversight of the Intelligence, Surveillance and Security Service Section 11 subsection 1 letter a. In its oversight of NIS, the Committee focuses in particular on ensuring that the service does not violate the statutory prohibition against monitoring or in any other covert manner procuring information concerning Norwegian physical or legal persons on Norwegian territory, cf. the Intelligence Service Act Section 4 first paragraph. In its inspection of NIS, the Committee oversees the following:

- The service's technical information collection
- The service's exchange of information with cooperating domestic and foreign services
- The service's computer systems
- Cases submitted to the Ministry of Defence and internal approval cases.[48]

During the inspections, the Committee is regularly briefed about NIS's ongoing activities, including the service's cooperation cases with other EOS services, the threat situation and cases submitted to the Ministry of Defence, as well as internal approvals. Such approvals can authorise surveillance or disclosure of information about Norwegian legal persons to foreign partners. For example, such approvals can give NIS internal authorisation to monitor a Norwegian national's communication equipment when the person is abroad. The legislation does not require external permission from the courts in such cases in the way it does for PST in relation to e.g. communications control.

Another key oversight point for the Committee is to oversee that the service complies with the Ministry of Defence's provisions regarding procurement of information concerning Norwegian persons outside Norwegian territory, and that it otherwise respects human rights as stipulated in the European Convention on Human Rights (ECHR), including ECHR Article 8 concerning the right to respect for private life.

In 2016, as in previous years, NIS briefed the Committee about non-conformities relating to its technical information collection. The Committee has asked follow-up questions in connection with one of these cases, and will provide information about the outcome of the investigation in next year's annual report.

In 2016, the Committee has kept informed about developments in the service's technical systems, installations and capacities. The Committee's technologist and technical expert have had several meetings with NIS in 2016 for the purpose of improving the EOS Committee's technical understanding in this area. This competence-building will be very important to the Committee's ability to understand the technical developments in the service and maintain effective oversight of NIS's activities in future.

7.2 Special report concerning the legal basis for NIS's surveillance activities

In the annual report for 2015, the EOS Committee stated that it would submit a special report to the Storting concerning the legal basis for NIS's surveillance activities. This report was submitted to the Storting on 17 June 2016. The Committee was of the opinion that actual, technological and legal developments that have taken place since the Intelligence Service Act was adopted constitute grounds for notifying the Storting of a potential need to amend the Norwegian Intelligence Service's regulatory framework.

The Standing Committee on Scrutiny and Constitutional Affairs submitted its recommendation to the Storting on 31 January 2017[49] in which it proposed that the Storting adopt the following resolution:

> 'The Storting asks the Government to submit a proposal for amendment of the Act relating to the Norwegian Intelligence Service.'

Since submitting the special report, the EOS Committee has overseen NIS as usual and in accordance with the description of the oversight arrangements provided in the special report. The Committee will continue to do so in 2017.

7.3 The Committee's right of access in the NIS

Extensive accounts of the Committee's right of access in the NIS have been provided in previous annual reports. Pursuant to the Oversight Act Section 4, the Committee may 'demand access to the administration's archives and registers,

48 Cf. the Royal Decree of 31 August 2001 No 1012 relating to instructions for the Norwegian Intelligence Service Section 13 letter d stating that 'matters of particular importance or that raise questions of principle' shall be submitted to the Ministry of Defence for consideration.

49 Recommendation No 164 to the Storting (2016–2017).

premises, and installations of all kinds'. The Storting made a plenary decision in 1999 stating that a special procedure shall apply for disputes about access to NIS documents. The decision did not lead to any amendments being made to the Act or Directive governing the Committee's oversight activities.[50] The Storting's 1999 decision was based on the particular sensitivity associated with NIS's human sources, the identity of persons with roles in occupational preparedness and particularly sensitive information received from cooperating foreign services.

In 2013, the EOS Committee asked the Storting to clarify whether the Committee's right of access as enshrined in the Act and Directive shall apply in full also in relation to NIS, or if the Storting's decision from 1999 shall be upheld. At the request of the Storting, this matter was considered in the report of the Evaluation Committee for the EOS Committee, submitted to the Storting on 29 February 2016.[51] Following a discussion, the Evaluation Committee concluded as follows:

> 'In light of this, the Evaluation Committee proposes that the EOS Committee be given an unconditional right of access also to the Norwegian Intelligence Service's particularly sensitive information, however, such that the Committee's duty to balance the need for oversight against considerations of national security, protection of sources and cooperation with other countries applies more stringently. Within the scope of such a solution, the current arrangement whereby particularly sensitive information is withheld from the EOS Committee's right to conduct free searches can be maintained such that access is only granted at the Committee's request. The Evaluation Committee also proposes that access only be granted to the chair and deputy chair of the EOS Committee. These two can decide whether to express criticism in cases involving particularly sensitive information. Moreover, the chair and deputy chair must agree in order for criticism to be expressed in such cases. The general rule that the Committee decides what to seek access to and the scope and extent of the oversight should, in the Evaluation Committee's view, also apply here.'

The Storting's Standing Committee on Scrutiny and Constitutional Affairs made the following comment in its recommendation[52] to the Evaluation Committee's report:

> 'The Committee notes that the Evaluation Committee is discussing the limitations on the EOS Committee's access to the Norwegian Intelligence Service. In principle, the Committee has full right of access, but what is called 'particularly sensitive information' is exempt. The Evaluation Committee proposes that the chair and deputy chair of the EOS Committee should be given access also to this information. In the Committee's opinion, this arrangement would result in an unfortunate division of the EOS Committee that would leave some members less able to carry out oversight than others.
>
> It is the view of the majority of the Committee, which comprises the whole Committee except the member from the Socialist Left Party, that the limitation on access to 'particularly sensitive information' must be resolved either by giving the whole EOS Committee access or by upholding the current arrangement based on the Storting's decision from 1999. The majority is of the opinion that the current arrangement of unclassified transparent criteria for which parts of the activities of the Norwegian Intelligence Service are exempt from continuous democratic oversight should continue. The majority also emphasises that the Committee must have the possibility to access cases in this category when it receives complaints.'

It is also stated in the recommendation that representatives on the Committee will submit a proposal for amendment of the Oversight Act to the Storting in the form of a private member's motion. The Evaluation Committee's proposals for amendment will then be considered in more detail.

The EOS Committee will continue its practice of requesting that NIS routinely informs the Committee about the number of cases and amount of data exempted from the Committee's right of access, as well as which of the four categories of the above-mentioned definition the case falls into. By 'particularly sensitive information' is meant:

1. The identity of the human intelligence sources of NIS and its foreign partners
2. The identity of foreign partners' specially protected civil servants
3. Persons with roles in and operational plans for occupational preparedness
4. NIS's and/or foreign partners' particularly sensitive intelligence operations abroad* which, if they were to be compromised,
    a. could seriously damage the relationship with a foreign power due to the political risk involved in the operation, or
    b. could lead to serious injury to or loss of life of own personnel or third parties.

*By 'intelligence operations abroad' is meant operations targeting foreign parties (foreign states, organisations or individuals), including activities relating to such operations that are prepared and carried out on Norwegian territory.

As mentioned in last year's annual report, NIS adopted *Guidelines for the processing of particularly sensitive information* in 2015. Among other things, these guidelines state that if information can no longer be regarded as particularly sensitive, it shall no longer be categorised as such and

shall be made available for the Committee's oversight. Such decategorisation of particularly sensitive information shall be considered once an operation has been concluded and subsequently at regular intervals. NIS decategorised four operations in 2016. These operations were consequently made available for oversight by the Committee.

The EOS Committee takes a positive view of the fact that through its guidelines, NIS demonstrates the ability and willingness to establish procedures to ensure that exemptions from the Committee's right of access do not exceed what is justified by the grounds provided. This enhances the democratic oversight of the service.

As described in the Committee's annual report for 2015, NIS had further improved and facilitated the Committee's independent searches. In 2016, NIS has immediately complied with the EOS Committee's requests for access to systems. The Committee is satisfied with how NIS facilitates the Committee's access and oversight.

7.4 NIS's access to the National Population Register

The Committee has raised certain issues with NIS relating to the service's access to public registers. The Committee has for some time been concerned with the issue of deletion of persons from the service's information collection system, as well as with how and when the service identifies a person as Norwegian and which investigative steps the services takes in connection with this. Section 4 of the Intelligence Service Act prohibits the procurement of information concerning Norwegian persons in Norway.

In 2012, NIS informed the Committee that the service does not have access to the National Population Register. The reason for the Committee's interest in this matter is that it is of the opinion that it will constitute less of a violation of a person's integrity if the service conducts searches in the National Population Register rather than procure information about the person, an action that could be illegal if the person is Norwegian or is in Norway.

Neither the Intelligence Service Act, the Intelligence Service Instructions or the pertaining preparatory works say anything about what degree of probability is required to decide whether a person is Norwegian or not and whether a person is on Norwegian territory. The Committee is of the opinion that searches in the National Population Register could be a crucial factor in determining a person's nationality.
In its concluding statement in the case, the Committee encouraged NIS to ask the Ministry of Defence for access to the National Population Register, cf. the Directive relating to Oversight of the Intelligence, Surveillance and Security Service Section 7 final paragraph. In its reply to the Committee, NIS stated that, following dialogue with the Ministry, the service was reconsidering the question of access to the National Population Register. Based on this assessment, the service concluded that access to the National Population Register is not deemed necessary at present. The Committee has taken note of this point of view.

7.5 Proposal from NIS

NIS proposed preparing a possible exception from the Intelligence Service Act Section 4 first paragraph for emergency situations and times of war pursuant to Section 3 first paragraph of the Act relating to Special Measures in Time of War, Threat of War and Similar Circumstances for a political decision if the situation so requires, and limited to necessary measures to procure information to support the defence fight. On this basis, the Committee asked whether it will be satisfactory for exceptions to be regulated in any other way than through the Storting's consideration of any excepting provisions in the Intelligence Service Act. The Committee's point of departure was that general authorisation provisions will not necessarily in themselves provide sufficient predictability for Norwegian citizens.

NIS later stated that its proposal to introduce such a provision as a potential part of the Emergency Preparedness System for the Armed Forces (BFF) has so far not been implemented by the Ministry of Defence, but that this does not mean that it is out of the question for this measure to be introduced following a concrete assessment and a political decision in a concrete emergency.

In its concluding letter to the service, the Committee maintained its view that any potential exceptions from NIS's legal framework under given scenarios should be regulated in law, and that it was somewhat difficult to see what crucial difference any statutory regulation in isolation would make to the Government's freedom of action compared with NIS's proposal. Should NIS's proposal become relevant again, the Committee assumes that its opinions will be taken into consideration in an overall assessment.

50 See Document No 16 (1998–1999), Recommendation No 232 to the Storting (1998–1999) and minutes and decisions by the Storting from 15 June 1999.

51 See Document 16 (2015–2016).

52 Recommendation No 146 to the Storting (2016–2017).

8.
Oversight of other EOS services

Photo: Forsvaret

8.1 General information about the oversight

The Committee continuously oversees intelligence, surveillance and security service carried out by, under the control of or on the authority of public authorities.[53] 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 Section 11 subsection 2 letter e, the Committee shall carry out annual inspections of at least two Intelligence Service units and/or intelligence/security service at military units, and of the personnel security service of at least two ministries/government agencies.

In 2016, the Committee inspected the security and intelligence functions at the Royal Norwegian Navy's main base (Haakonsvern) and the Norwegian Armed Forces' Joint Headquarters (NJHQ). The Committee also inspected the NIS unit at the Norwegian Armed Forces' Joint Headquarters (NJHQ). In addition, the Committee inspected the personnel security services of the National Police Directorate and the County Governor of Rogaland.

The above-mentioned inspections were prepared in advance by the Committee Secretariat, among other things by searches in computer systems. Neither of the inspections of the NJHQ, the NIS unit at NJHQ, the Police Directorate and the County Governor of Rogaland gave grounds for follow-up or criticism.

The follow-up of the Committee's inspection of Haakonsvern is described in more detail in section 8.2.

8.2 Follow-up of inspection of the Royal Norwegian Navy's main base Haakonsvern

The Committee inspected the intelligence and security functions at the Royal Norwegian Navy's main base Haakonsvern (SHH) in September 2016. During the inspection, the Committee noted a list of persons who were to be denied entry to the base, and the list included their national identity numbers and photos. The Committee asked SHH whether the base had procedures in place to ensure compliance with the requirements concerning processing of personal data stipulated in the Personal Data Act,[54] cf. the Personal Data Act Section 14.

In its reply, SHH gave an account of how the no entry list is practised. It was stated that no guidelines exist for when persons are to be removed from the list, and that it is revised at irregular intervals.

When concluding the case, the Committee urged SHH to establish procedures that comply with the above-mentioned provisions. Establishing such procedures will help to ensure that the processing of personal data on the no entry list meets the applicable statutory requirements.

During the inspection, the Committee also noticed that some completed personal particulars forms and declarations of secrecy relating to security clearance cases lay unorganised in an archive. The Committee referred to the requirements set out in the Regulations concerning Personnel Security Section 6-3 for documents to be kept in a separate case folder. The Committee noted that SHH will consider its procedures for filing of documents based on this, and urged the base to bring its procedures into compliance with the requirements of the Regulations.

The Committee requested feedback from SHH on measures taken, cf. the Directive relating to Oversight of the Intelligence, Surveillance and Security Service Section 7 final paragraph. The Committee will return to the results, if any, of the Committee's request in next year's annual report, cf. the Directive relating to Oversight of the Intelligence, Surveillance and Security Service Section 13 (3) letter e.

53 Cf. the Oversight Act Section 1 first paragraph.

54 An assessment must be made to determine whether the processing is necessary, whether the information is adequate and relevant, and information must not be stored for longer than required to fulfil the purpose of the processing, cf. the Personal Data Act Section 8 and Section 11 letters d) and e).

9.
External relations and administrative matters

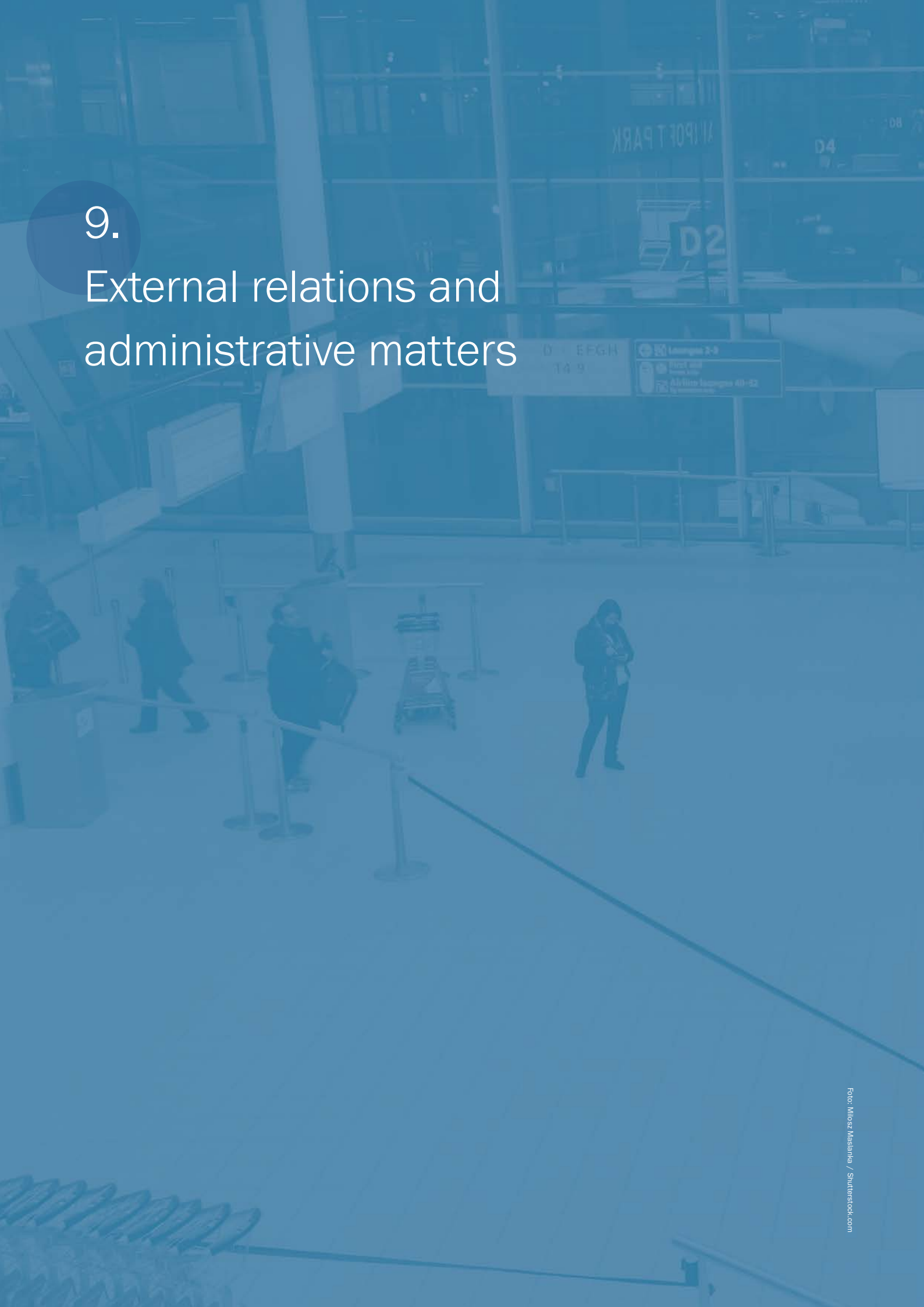


Foto: Miłosz Maslanka / Shutterstock.com

9.1 The Committee's external relations

The EOS Committee has had extensive contact with relevant external environments in 2016. These environments include other states' oversight bodies, research communities in Norway and abroad and national supervisory agencies. It is important for the Committee to have transparency regarding its work.

The Committee marked its 20th anniversary in 2016. The anniversary was held over two days and represented a good opportunity to make contact with external parties and environments, reflect on past developments and look ahead. The Committee organised a scientific conference held in English and an anniversary seminar. The scientific conference day attracted broad international participation and formed the basis for an ongoing project on how oversight of the secret services is influenced by international political trends. The legal research community at Durham University in England is also contributing to this project. The anniversary seminar targeted a Norwegian audience. The Committee welcomed representatives of the Storting, the Government and the EOS services, along with colleagues from the Nordic countries, scholars and other representatives of civil society. The EOS Committee intended this seminar to mark 20 years of democratic oversight of the Norwegian EOS services.

The EOS Committee frequently receives enquiries from Norwegian and foreign representatives who wish to learn more about the oversight of the EOS services in Norway. In addition, the Committee and the Secretariat take the initiative in relation to other external parties and environments and seek to develop their knowledge and oversight methods.

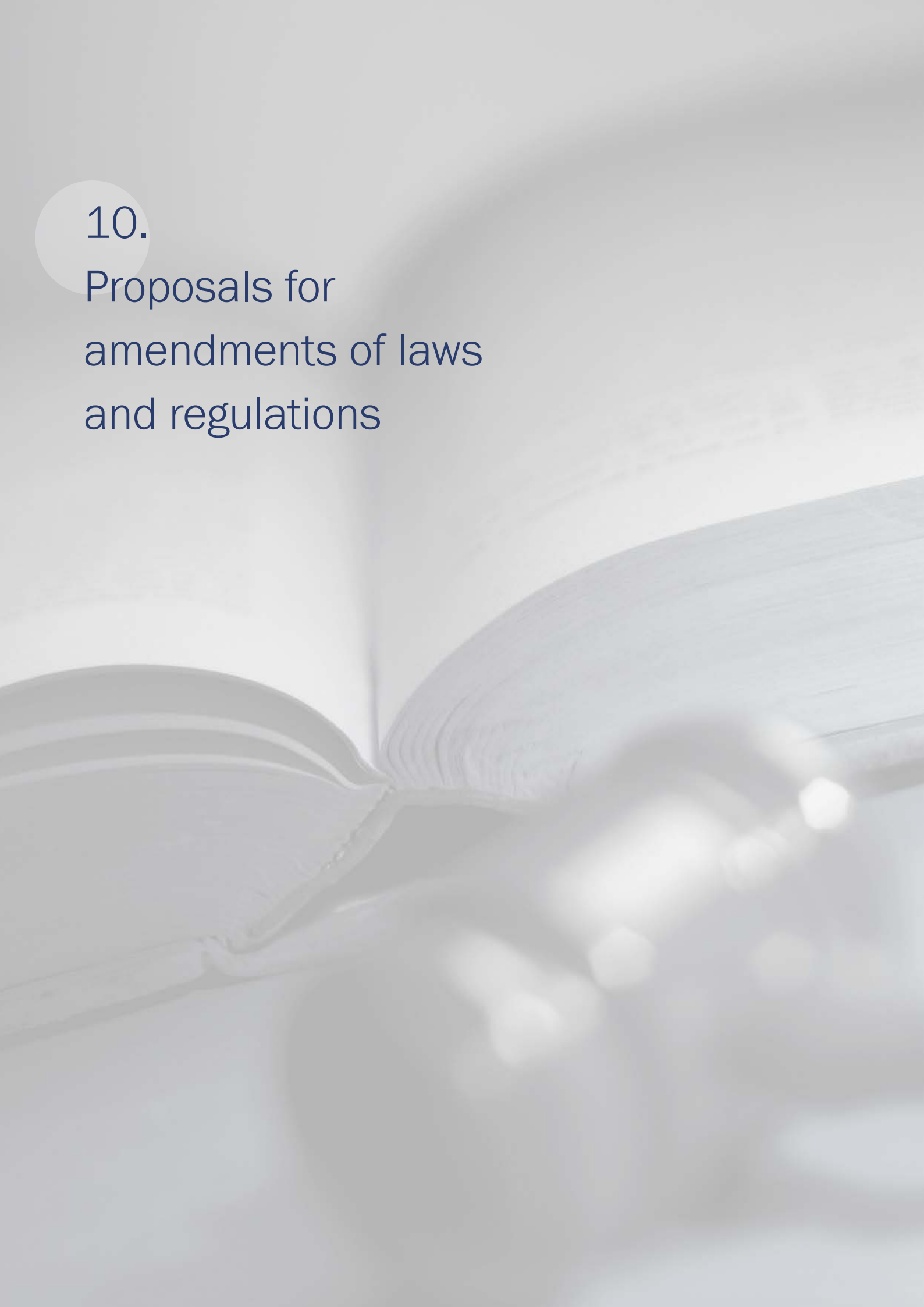
In 2016, the Committee and the Secretariat attended and organised meetings, visits, conferences etc. An overview of these events is provided in appendix 2.

9.2 Administrative matters

The Committee's expenses amounted to NOK 14,764,958 in 2016, compared with a budget of NOK 14,950,000, including transferred funds. The Committee has applied for permission to transfer the unused portion of its allocations to the budget for 2017. As mentioned in last year's annual report, the Committee needs to move to bigger and more secure premises. The Committee continues its work to define requirements for satisfactory premises. The Storting is kept informed about the matter. A lot of time has been spent in 2016 on the planning of new premises, and this work will continue in 2017. The Committee expects to incur greater planning costs in 2017. There is still a need to expand the Secretariat by hiring more staff. The Committee will return to this matter in connection with the budget process for 2018.

The Committee concludes that the National Security Authority (NSM) continues to take an unreasonably long time to grant security clearance to secretariat staff. When new employees do not have security clearance when they take up the position, the Committee has to pay their wages, but cannot use their labour. The Committee's oversight activities suffer, and this creates what is, in the Committee's opinion, a most unusual situation.

10.
Proposals for amendments of laws and regulations



The EOS Committee hereby gives notification of a potential need to change the regulatory framework, cf. the Directive relating to Oversight of the Intelligence, Surveillance and Security Service Section 13 (3) letter h.

The oversight of security clearance cases in 2016 has given grounds for the Committee to consider whether the Committee should have the right to express to the public administration that compensation should be paid to individuals for errors committed by the administration.[55] This is not a possibility under the current Oversight Act. In this connection, there is reason to consider the Act concerning the Storting's Ombudsman for Public Administration.[56]

Like the Ombudsman for Public Administration, the EOS Committee is a Storting-appointed body, and the EOS Committee's activities are based on many of the principles that are enshrined in the Act concerning the Storting's Ombudsman for Public Administration. The Act states the following in Section 10 third paragraph on *Completion of the Ombudsman's procedures in a case*:

> 'If the Ombudsman finds that there are circumstances that may entail liability to pay compensation, he may, depending on the situation, suggest that compensation should be paid.'

The Directive relating to Oversight of the Intelligence, Surveillance and Security Service Section 7 stipulates which principles from Section 10 of the Act concerning the Storting's Ombudsman for Public Administration the Committee shall base its oversight and the formulation of its statements on, but this does *not* include the paragraph quoted above. The question is then whether the EOS Committee is *prevented from* suggesting that compensation should be paid in a case.

The EOS Committee exercises parliamentary-based oversight, which, constitutionally speaking, entails real independence in relation to the services subject to its oversight. It is expressly stated in the Oversight Act Section 2 that the purpose of the EOS Committee is purely to oversee, and that it may not instruct the bodies it oversees. The sanctions available to the Committee is then limited to criticism and statements of opinion, and does not include issuing instructions to the public administration. This is a parallel to the Parliamentary Ombudsman's oversight function.

The preparatory works to the Act concerning the Storting's Ombudsman for Public Administration state that, in connection with a statement that the public administration has made an error, the Parliamentary Ombudsman 'must (...) also have the possibility to suggest to the public administration that compensation should be paid if the matter cannot be remedied by a new decision'.[57] Subsequent amendments to the Act concerning the Storting's Ombudsman for Public Administration have not involved any comments on the provision concerning compensation.[58] Based on the above, there does not seem to be any constitutional obstacles to such statements being made by the Storting's oversight bodies. However, considering the express regulation in the Act concerning the Storting's Ombudsman for Public Administration and corresponding lack thereof in the Oversight Act, the Committee is of the opinion that it currently falls outside the scope of its remit to suggest that compensation should be paid as a consequence of errors on the part of the public administration.

There are good reasons why the means available to the EOS Committee and the Parliamentary Ombudsman differ on some points. Nevertheless, the Committee's processing of complaints concerning security clearance decisions is a perfect parallel to the complaints that the Parliamentary Ombudsman receives concerning final decisions made by the public administration.

The possibilities open to complainants in the Parliamentary Ombudsman's area of responsibility are not open to people who submit complaints concerning security clearance cases to the EOS Committee. The Committee questions whether this difference is justified.

Former Parliamentary Ombudsman for Public Administration Arne Fliflet concluded that 'the Storting's Ombudsman arrangement can be a useful supplement and alternative to the courts in cases involving claims for compensation from public authorities'.[59] Fliflet writes that the Parliamentary Ombudsman can 'use recommendations to pay compensation as a means of remedying errors and preventing citizens from suffering injustices at the hands of the public administration'.[60]

55 See sections 5.7 and 5.8.2. This also concerns cases where processing was not completed in 2016.

56 Act No 8 of 22 June 1962 concerning the Storting's Ombudsman for Public Administration.

57 See Proposition No 30 to the Odelsting (1959–1960), page 21.

58 Arne Fliflet, *Sivilombudsmannen og behandlingen av saker om offentlig erstatningsansvar*, in Bonus Pater Familias; Festschrift on the occasion of Peter Lødrup's 70th birthday, page 273, Gyldendal Akademisk 2002.

59 Arne Fliflet, *Sivilombudsmannen og behandlingen av saker om offentlig erstatningsansvar*, in Bonus Pater Familias; Festschrift on the occasion of Peter Lødrup's 70th birthday, page 273, Gyldendal Akademisk 2002.

60 Arne Fliflet, *Sivilombudsmannen og behandlingen av saker om offentlig erstatningsansvar*, in Bonus Pater Familias; Festschrift on the occasion of Peter Lødrup's 70th birthday, page 273, Gyldendal Akademisk 2002.

The Committee exercises oversight in security clearance cases in far fewer cases than the number of complaint cases processed by the Parliamentary Ombudsman. However, these cases are extremely important to the persons concerned, and can be vital to their professional career.

It is an important factor here that the processing of security clearance cases remains a partly closed process that is not subject to the same right of access as other public administration cases. This represents an obstacle to the right of individuals to bring legal action on the basis of errors made by a security clearance authority, for example because they have not been given detailed grounds for the decision or been granted access to documents. Fliflet points out that 'bringing civil action against the public administration will rarely be seen as a realistic means of having any injustice or errors committed remedied'.[61] This consideration will apply just as much, if not more, in security clearance cases.

The Committee requests that the Storting consider whether it should be enshrined in law that the Committee should be entitled to make statements about the public administration's liability in damages. In the event that the Storting is of the opinion that the EOS Committee can make statements about the public administration's liability in damages, it can also be considered whether this should trigger a right to free legal representation without means testing if the public administration does not comply with the Committee's statement in the question of compensation. Pursuant to Act No 35 of 13 June 1980 relating to Free Legal Aid Section 16 first paragraph (3), the 'private party' is entitled to 'free legal representation (...) without means testing' in cases where a lawsuit is recommended by the Parliamentary Ombudsman.

61 Arne Fliflet, *Sivilombudsmannen og behandlingen av saker om offentlig erstatningsansvar*, in Bonus Pater Familias; Festschrift on the occasion of Peter Lødrup's 70th birthday, page 273, Gyldendal Akademisk 2002.

11. Appendices

Appendix 1 – Definitions

Authorisation
Decision to grant a person with security clearance access to information with a specified security classification.

Averting investigation
Investigation for the purpose of preventing a criminal act from being committed.

Classified information
Information that shall be protected for security reasons pursuant to the provisions of the Security Act. This information shall be marked with a security classification, for example CONFIDENTIAL.

Computer script
A script is a computer program that is designed to e.g. automatically identify registrations that are ready for a manual review in accordance with the five-year rule.

Covert coercive measures
Investigation methods whose use the suspect is unaware of, for example communications control, covert audio surveillance and secret searches.

Drop a case
A decision that a case will be concluded without a decision being made based on the merits of the case.

Folder structure
Windows Explorer can be used to view the folder structure of a hard disk/network station, including all files processed there, for example the I area.

FSA computer network
A dedicated case processing system for the FSA's operational work outside the area of personnel security.

Incident that poses a threat to security
Activity that poses a threat to security, sensitive information being compromised and serious security breaches.

Information processing
Any form of electronic or manual processing of information.

Intelligence register
Register of intelligence information that is deemed necessary and relevant for PST in the performance of its duties. PST uses the intelligence register Smart.

Intelligence registration
Processing of information that is deemed necessary and relevant for PST in the performance of its duties, and that does not warrant opening of or processing in a prevention case.

Internal grounds (ISB)
An internal document that security clearance authorities are obliged to prepare in connection with security clearance decisions. This document must deal with all the material factors in the case, including the provisions on which the decision is based, the matters to which importance has been attached pursuant to Section 21 of the Security Act, and which facts the decision is based on.

Investigation case
Case opened for the purpose of investigating whether a criminal offence that falls within PST's area of responsibility has taken place.

Mimir
Case processing tool used in security clearance cases.

Observation period
Decision regarding when a request for a person to be granted security clearance may be resubmitted.

Particularly sensitive information
By 'particularly sensitive information', cf. NIS's *Guidelines for the processing of particularly sensitive information*, is meant:

1. The identity of the human intelligence sources of NIS and its foreign partners
2. The identity of foreign partners' specially protected civil servants
3. Persons with roles in and operational plans for occupational preparedness
4. NIS's and/or foreign partners' particularly sensitive intelligence operations abroad* which, if they were to be compromised,
   a. could seriously damage the relationship with a foreign power due to the political risk involved in the operation, or
   b. could lead to serious injury to or loss of life of own personnel or third parties.

*By 'intelligence operations abroad' is meant operations targeting foreign parties (foreign states, organisations or individuals), including activities relating to such operations that are prepared and carried out on Norwegian territory.

Personal data
Information or assessments that can be linked to an individual.

Personnel security
Measures, actions and assessments made to prevent persons who could constitute a security risk from being placed in a situation that makes the risk more immediate.

Prevention case
Case opened for the purpose of investigating whether someone is preparing to commit a criminal offence that PST is tasked with preventing.

Requesting authority
A body that, as or on behalf of an authorising authority, requests vetting of personnel.

Restriction of access to information
Marking of registered information for the purpose of limiting future processing of the information in question, cf. the Police Register Act Section 2 subsection 10.

Security clearance
Decision made by a security clearance authority regarding a person's presumed suitability for a specified security classification.

Security clearance authority
Public body authorised to decide whether or not people should be granted security clearance.

Security clearance case
Case concerning a decision to grant or deny security clearance, requires an assessment of the person's suitability.

Security interview
Interview conducted by the security clearance authority in order to assess a person's suitability in a security clearance case.

SIS
Schengen Information System (SIS).

Smart
PST's intelligence register.

Smartsak
PST's tool for prevention cases and investigation cases.

The five-year rule
The requirement for PST's intelligence registrations to be re-evaluated if no new information has been added during the past five years.

Vetting
Obtaining information of relevance to the security clearance assessment.

Appendix 2 – Meetings, visits and participation in conferences etc.

Brief descriptions of meetings, visits, and conferences etc. that the Committee and the Committee Secretariat have participated in and organised in 2016 are provided below. In addition to the events listed below, the chair, other committee members and secretariat staff have also given talks on the EOS Committee's activities in some less formal contexts.

Visit to the Venice Commission and CODEXTER

In January 2016, two secretariat employees visited the Venice Commission and the Committee of Experts on Terrorism – the Council of Europe (CODEXTER). Both organisations are located in Strasbourg. This was part of the effort to increase knowledge about the ongoing international antiterrorism cooperation and developments in the oversight of EOS services in Europe.

Meeting with a scholar from the University of Buckingham

In February, the Secretariat met with Co-Director of the Centre for Security and Intelligence Studies at the University of Buckingham, Dr Julian Richards. The meeting was held to learn more about intelligence and surveillance activities from a recognised scholar in the field.

Meeting with a representative of the Danish Intelligence Oversight Board

In February, the Secretariat met with an employee of the Danish oversight body for the intelligence services. The purpose of the meeting was to exchange and learn from each other's experience and plan future activities.

Seminar in Geneva

In March, the chair, one committee member and a secretariat employee participated in a side event in connection with the United Nations Human Rights Council in Geneva. The seminar was held in connection with the international launch of the book Making International Intelligence Cooperation Accountable, and was held in cooperation with the Geneva Centre for the Democratic Control of Armed Forces (DCAF).

Visit by a delegation from the office of the Chancellor of Germany

In March, the Committee received visitors from the office of the Chancellor of Germany. The visit was part of a study trip to Norway lasting several days during which the German delegation wanted to learn more about the Norwegian oversight model for the EOS services.

Study trip to Berlin

In March, two secretariat employees visited representatives from German research environments, the office of the Chancellor and the Bundestag. The visit was part of the effort to increase knowledge of the ongoing reform of the legal basis for the German EOS services.

20th anniversary conference

In April, the EOS Committee hosted a scientific conference and an anniversary seminar to mark the Committee's 20th anniversary.

Meeting with other states' oversight bodies in the Hague, the Netherlands

In April, secretariat employees met with colleagues from several other states' oversight bodies in connection with an international project relating to democratic oversight of the services' exchange of personal data across national borders.

Visit to the Ukrainian parliament

In May, a committee member visited the Ukrainian parliament, Verkhovna Rada, to give a talk on the Norwegian oversight model for the EOS services. This visit was facilitated by DCAF.

Visit from the German Bundestag's Parliamentary Oversight Panel

In June, the Committee received a visit from the Bundestag's Parliamentary Oversight Panel ('G13'). The visit was part of a study trip to Norway lasting several days during which the German delegation wanted to learn more about the Norwegian oversight model for the EOS services.

Conference on intelligence and surveillance in Breda, the Netherlands

In June, a secretariat employee attended a conference where democratic oversight of secret services were among the topics discussed. The conference was organised by the International Association for Intelligence Education.

Visit to the Ukrainian parliament

In July, a secretariat employee attended a conference under the auspices of the Ukrainian parliament, Verkhovna Rada, to give a talk on the Norwegian oversight model for the EOS services. The visit was facilitated by the Organization for Security and Co-operation in Europe (OSCE).

Meeting with judges from Oslo District Court who hold security clearances

In August, the Secretariat met with two Oslo District Court judges who hold security clearances. The meeting was held to exchange knowledge about each other's roles and duties in relation to PST's petitions to the court for authorisation to use covert coercive measures etc.

Meeting with other states' oversight bodies in Brussels, Belgium

In September, two secretariat employees met with colleagues from several other states' oversight bodies in Brussels in connection with an international project relating to improving democratic oversight of the services' exchange of personal data across national borders.

Intelligence conference, Vadsø

In October, the chair of the Committee gave a presentation about the EOS Committee, its composition, tasks and remit at the intelligence conference in Vadsø.

Conference in Belgrade, Serbia

In October, a committee member gave a talk at Belgrade Security Forum's conference on security in democracies. The topic of the presentation was the EOS Committee's remit, structure and oversight of the EOS services in Norway.

Visit to Durham University, UK

In November, a secretariat employee met with researchers at Durham University as part of the follow-up of the scientific research project relating to the first day of the 20th anniversary event in April.

Lecture at the Norwegian Defence Command and Staff College

In November, the chair of the Committee and a secretariat employee gave a lecture on the EOS Committee and democratic oversight of EOS services as part of the college's course on politics, society and intelligence.

Meeting with other states' oversight bodies in the Hague, the Netherlands

In November, two secretariat employees met with colleagues from several other states' oversight bodies in the Hague in connection with an international project relating to democratic oversight of the services' exchange of personal data across national borders.

Meeting with the Swedish inspection authority for military intelligence activities

In November, several secretariat employees met with colleagues from the Swedish oversight body Statens inspektion för försvarsunderrättelseverksamheten (SIUN). The purpose of the visit was to exchange knowledge about oversight tasks, particularly in relation to the Swedish oversight of

the Swedish National Defence Radio Establishment's (FRA) signal intelligence and the Norwegian digital border control (DGF) proposal.

Appendix 3 – Act relating to Oversight of Intelligence, Surveillance and Security Service[62]

Section 1. The oversight committee and the oversight area

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

Such oversight shall not apply to any superior prosecuting authority.

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

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

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

Section 2. Purpose

The purpose of the oversight is:

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

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

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

Section 3. The responsibilities of the Oversight Committee

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

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

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

Section 4. Right of access, 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. The Committee's right of inspection and access pursuant to the first sentence shall apply correspondingly in relation to enterprises that assist in the performance of intelligence, surveillance, and security services.

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

Section 5. Statements, obligation to appear, etc.

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

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

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

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

The Committee may apply for a judicial recording of evidence pursuant to Section 43, second subsection, of the Courts of Justice Act. Sections 22-1 and 22-3 of the Civil Procedure Act shall not apply. Court hearings shall be held

in camera and the proceedings shall be kept secret. The proceedings shall be kept secret until the Committee or the competent ministry decides otherwise, cf. Sections 8 and 9.

Section 6. Ministers and ministries

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

Section 7.

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

Section 8. Statements and notifications

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

   The Committee shall decide the extent to which its unclassified statements or unclassified parts of statements shall be made public. If it is assumed that making a statement public will result in revealing the identity of the complainant, the consent of this person shall first be obtained.
2. The Committee submits annual reports to the Storting about its activities. Such reports may also be submitted if factors are revealed that should be made known to the Storting immediately. Such reports and their annexes shall be unclassified.

Section 9. Duty of secrecy, etc.

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

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

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

Section 10. Assistance etc.

The Committee may engage assistance.

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

Section 11. Penalties

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

Section 12. Entry into force

This Act shall enter into force immediately.

Appendix 4 – Directive relating to Oversight of Intelligence, Surveillance and Security Service[63]

§ 1. On the Oversight Committee and its secretariat

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

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

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

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

62 Act No 7 of 3 February 1995 relating to the Oversight of Intelligence, Surveillance and Security Services (the Oversight Act)

63 Directive relating to Oversight of the Intelligence, Surveillance and Security services, adopted by a Storting resolution of 30 May 1995.

Section 2. Quorum and working procedures

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

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

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

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

Section 3. Procedure regulations

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

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

Section 4. Oversight limitations etc.

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

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

Section 5. Access limitations

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

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

Section 6. Disputes concerning access to information and oversight

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

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

Section 7. On the oversight and statements in general

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

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

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

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

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

Section 8. On complaints

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

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

If a complaint contains valid grounds for criticism or

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

Section 9. Procedures

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

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

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

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

Section 10. Investigations at the ministries

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

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

Section 11. Inspection

1. Responsibilities for inspection are as follows:

a) For *the intelligence service*: to ensure that activities are carried out within the framework of the service's established responsibilities, and that no injustice is done to any person.

b) For *the National Security Authority*: to ensure that activities are carried out within the framework of the service's established responsibilities, to oversee clearance matters in relation to persons and enterprises for which clearance has been denied, revoked, reduced or suspended by the clearance authorities, and also to ensure that no injustice is done to any person.

c) For *the Police Security Service*: to oversee that the service's handling of preventive cases and investigations, its use of concealed coercive measures, its processing of personal data, and the exchange of information with domestic and foreign collaborative partners is carried out in accordance with current regulations, and meets the requirements for satisfactory routines within the framework of the purpose stated in Section 2 of the Act.

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

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

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

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

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

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

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

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

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

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

Section 12. Information to the public

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

mentioning specific persons, consideration shall be given to protection of privacy, including persons not issuing complaints. Civil servants shall not be named or in any other way identified except by authority of the ministry concerned.

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

Section 13. Relationship to the Storting

1. The provision in Section 12, first subsection, correspondingly applies to the Committee's notifications and annual reports to the Storting.
2. Should the Committee find that the consideration for the Storting's supervision of the administration dictates that the Storting should familiarise itself with classified information in a case or a matter the Committee has investigated, the Committee must notify the Storting specifically or in the annual report. The same applies to any need for further investigation into matters which the Committee itself cannot pursue further.
3. By 1 April every year, the Committee shall report its activities in the preceding year to the Storting.
   The annual report should include:
   a) an overview of the composition of the Committee, its meeting activities and expenses.
   b) a statement concerning implemented supervision activities and the result of said activities.
   c) an overview of complaints by type and service branch, indicating what the complaints resulted in.
   d) a statement concerning cases and matters raised on the Committee's own initiative.
   e) a statement concerning any measures the Committee has requested be implemented and what these measures led to, cf. Section 6, fifth subsection.
   f) a statement concerning any protests pursuant to Section 5.
   g) a statement concerning any cases or matters which should be put before the Storting.
   h) the Committee's general experiences from the oversight activities and the regulations and any need for changes.

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

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

Appendix 5 – The EOS Committee's consultation submission concerning digital border control (DGF)

The Ministry of Defence
P.O. Box 8126 Dep.
NO-0032 OSLO

20 December 2016

Consultation submission from the EOS Committee – consultation concerning report submitted by the Lysne II Committee on digital border control

The EOS Committee refers to the Ministry of Defence's consultation letter of 5 October 2016 in connection with the consultation concerning the report submitted by the Lysne II Committee on digital border control.

In its report, the Lysne II Committee points out the many considerations that need to be discussed in connection with the possible introduction of digital border control (DGF), of which protection of privacy and human rights are key considerations. The conclusion arrived at by the Lysne II Committee is that DGF 'can be introduced in a manner than combines consideration for technologically feasible solutions, legal acceptability, protection of privacy issues, intelligence value and public confidence'.

The Lysne II Committee has proposed an oversight system consisting of the following elements:

- Advance court approval (the DGF court)
- A supervisory authority that monitors the use of DGF in near-real time (the DGF supervisory authority)
- Strengthening of subsequent oversight by the EOS Committee

The grounds given for establishing a DGF supervisory authority are the need for 'virtually continuous independent oversight, in near-real time, in connection with the implementation of the DGF system'. The proposed solution is to establish the DGF supervisory authority as an administrative body subordinate to a ministry other than the Ministry of Defence (the Ministry of Transport and Communications) in order to ensure its independence. It is proposed that the supervisory authority shall:

- In near-real time receive all information about all searches conducted in data collections in the DGF system, receive all the DGF court's decisions, have access to information about the implementation and configuration of filters, and have access to all information about how internal guidelines and court decisions have been translated into search privileges
- Report non-conformities to the EOS Committee and otherwise report regularly to the EOS Committee, the Ministry of Defence and the Ministry of Transport and Communications
- Supervise that data security in the DGF system is as stringent as is technologically and practically possible

As regards reporting to the EOS Committee by the DGF supervisory authority, the Lysne II Committee writes:

> 'In the Committee's opinion, the DGF supervisory authority should not be authorised to stop activities or publicly criticise the Norwegian Intelligence Service for breaches of the regulatory framework for DGF. This will necessitate establishing legal expertise that will duplicate the EOS Committee's expertise, and it will also create inexpedient lines of responsibility in relation to the EOS Committee's remit. The Committee is therefore of the opinion that the supervisory authority should immediately report any suspicion of non-conformities to the EOS Committee, which will consider follow-up measures in line with the Committee's powers and report to the Storting in accordance with established practice.'

The EOS Committee has no opinion about whether or not DGF should be introduced in Norway, nor about the conditions for using this method.

The Committee would like to make the following statement in relation to the Lysne II Committee's proposal for oversight of DGF:

The Storting established the EOS Committee for the purpose of conducting an overall review of the legality of the EOS services. If a DGF supervisory authority is established, this will mean that the EOS Committee's oversight of this method would be indirect, as opposed to the direct oversight that the EOS Committee currently exercises of the EOS services, including the Norwegian Intelligence Service.

The EOS Committee would like to point out that all reporting from the proposed DGF supervisory authority to the EOS Committee will to a certain extent have to be based on discretionary judgement, particularly in terms of what is deemed to constitute a non-conformity. The proposed solution, with a supervisory authority that is subordinate to a ministry, could in practice mean that the exercise of discretion with respect to what is reported to the EOS Committee will not be subject to parliamentary oversight. It will probably fall outside the EOS Committee's area of oversight to oversee a DGF supervisory authority, cf. the Oversight Act[64] Section 1 first paragraph. Pursuant to the Act Section 3 final paragraph, the Committee's investigations 'may exceed the framework defined in Section 1, first paragraph' 'when this serves the clarification of matters or factors that the Committee investigates by virtue of its mandate'. The decisions of the Committee concerning such matters 'shall be binding on the administration' pursuant to the Directive relating to Oversight of the Intelligence, Surveillance and Security Services[65]. If a DGF supervisory authority is established, the EOS Committee will have to consider whether it should, periodically or permanently, make such a decision on oversight of the DGF supervisory authority in order to be able to fulfill the purpose of the oversight, including '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', cf. the Oversight Act Section 2. It could otherwise be difficult for the EOS Committee to fulfill the oversight function that the Storting has assigned to the Committee in relation to DGF.

The EOS Committee's view is that it will in any case be necessary to draw clear boundaries between the EOS Committee and a DGF supervisory authority.

The Lysne II Committee appears to have considered whether the DGF supervisory authority's tasks could be assigned to the EOS Committee, and it concluded:

'In the Committee's opinion, it will probably be inexpedient, given the EOS Committee's role as a Storting-appointed oversight body and its statutory task of exercising subsequent oversight, for this task to be assigned to the EOS Committee'.

In the EOS Committee's opinion, it is not clear that the EOS Committee's parliamentary basis as an independent oversight body appointed by the Storting, and subsequent oversight, are factors that make the EOS Committee unfit to perform the tasks that the proposal assigns to a possible future DGF supervisory authority. The Committee's remit and independent responsibility to carry out oversight activities on behalf of the Storting will entail a need to strengthen the EOS Committee's technical expertise to oversee the DGF method, regardless of whether a separate DGF supervisory authority is established.

Since the DGF supervisory authority shall 'supervise that the activities are carried out in accordance with the law',[66] the EOS Committee concludes that the establishment of a supervisory authority will result in the duplication not only of technological expertise, but also legal expertise.

The EOS Committee also notes that the DGF supervisory authority will not be 'authorised to stop activity' that is unlawful etc. For purposes of comparison, the EOS Committee refers to the fact that Statens inspektion för försvarsunderrättelseverksamheten (SIUN), the Swedish oversight body for the Swedish signals intelligence act (the FRA Act), has the authority to make such decisions to stop activity. SIUN also has the authority to decide that unlawfully obtained material must be deleted/destroyed. The EOS Committee has no authority to order the EOS services to stop any activities that might be in breach of the law, court decisions, regulations or internal guidelines. Based on the above, it may be considered whether the authority to make decisions to stop information procurement activities and order the deletion of unlawfully procured material should be enshrined in the regulatory framework.

There is no doubt that the EOS Committee must be strengthened if DGF is introduced in line with the present proposal, and the Lysne II Committee proposes this in its report. However, the EOS Committee assumes that the introduction of DGF will require a substantial increase in resources, primarily in the form of more staff with technological expertise being employed by the Committee Secretariat.

Otherwise, the EOS Committee notes and agrees with the Lysne II Committee's assessments of the necessity of regulating DGF in law as an intelligence method. For purposes of comparison, the EOS Committee refers to the fact that the Swedish signals intelligence act (the FRA Act) regulates the Swedish National Defence Radio Establishment's (FRA) collection of signals *from all types of signal carriers*, not only signals transmitted via cables. In this connection, the EOS Committee refers to its special report to the Storting concerning the legal basis for the Norwegian Intelligence Service's surveillance activities, submitted on 17 June 2016. In this report, the EOS Committee highlighted a potential need to examine in more detail whether NIS should be given a clearer legal basis for all the methods it uses that interfere with the rights of individuals, with pertaining due process guarantees, based on the actual, technological and legal developments that have taken place since the Intelligence Service Act was adopted in 1998. In this connection, the EOS Committee raised the question of whether approval of the use of intrusive methods by NIS should be subject to court approval or similar in addition to the EOS Committee's external subsequent oversight.

If the proposal to introduce DGF as a method for NIS is enacted in law, the EOS Committee would like to raise the question of whether the other methods used by NIS should not also be subject to statutory regulation.

Yours sincerely,

Eldbjørg Løwer
Chair of the EOS Committee

64 Act No 7 of 3 February 1995 relating to the Oversight of Intelligence, Surveillance and Security Services (the Oversight Act).

65 Directive No 4295 of 30 May 1995 relating to Oversight of the Intelligence, Surveillance and Security Services.

66 The Lysne II Committee's report, page 52 second column.

Appendix 6 – Statistics concerning the Committee's activity 1996–2016

Year	Number of committee meetings	Complaint cases in total	Own initiative	Number of inspections
1996	17	34	Ingen	16
1997	17	58	18	22
1998	16	21	14	26
1999	24	17	5	22
2000	26	14	7	22
2001	25	25	10	21
2002	16	28	12	24
2003	19	22	10	24
2004	18	17	7	22
2005	19	14	18	23
2006	18	16	15	27
2007	20	22	18	28
2008	17	13	13	26
2009	14	27	20	27
2010	22	21	23	28
2011	26	29	16	23
2012	23	21	22	30
2013	21	47	26	28
2014	21	26	39	25
2015	19	23	37	25
2016	12[67]	32	51	26

67 Transition to longer committee meetings (full-day meetings).

NORWEGIAN PARLIAMENTARY OVERSIGHT COMMITTEE
ON INTELLIGENCE AND SECURITY SERVICES

Illustration: Mfreakon

fdesign.no

Contact information

Telephone: +47 23 31 09 30
Email: post@eos-utvalget.no
Postal address: PO box 84 Sentrum, N-0101 Oslo, Norway
Office address: Akersgata 8, Oslo

www.eos-utvalget.no