



NORWEGIAN PARLIAMENTARY
OVERSIGHT COMMITTEE
ON INTELLIGENCE AND SECURITY SERVICES



ANNUAL REPORT 2021

DOCUMENT 7:1 (2021-2022)

To the Storting

In accordance with Act No 7 of 3 February 1995 relating to the Oversight of Intelligence, Surveillance and Security Services (the Oversight Act) Section 17 third paragraph, the Committee hereby submits its report about its activities in 2021 to the Storting.

The annual report is unclassified, cf. the Oversight Act Section 17 third paragraph. Pursuant to the Security Act, the issuer of information decides whether it is classified. Before the report is submitted to the Storting, the Committee sends the relevant sections of the report to each of the respective services so that they can clarify whether the report complies with this requirement. The services have also been given the opportunity to check that there are no factual errors or misunderstandings in the text.

Oslo, 30 March 2022



Astri Aas-Hansen



Kristin Krohn Devold



Magnhild Meltveit Kleppa



Erling Johannes Husabø



Camilla Bakken Øvald



Jan Arild Ellingsen



Olav Lysne



Henrik Magnusson



The EOS Committee in 2021. From left: Camilla Bakken Øvald, Jan Arild Ellingsen, Olav Lysne, Astri Aas-Hansen (chair), Magnhild Meltveit Kleppa, Kristin Krohn Devold (deputy chair) and Erling Johannes Husabø. (Photo: Anki Grøthe)

Contents

1.	THE COMMITTEE'S REMIT AND COMPOSITION.....	5
2.	KEY FIGURES AND GOVERNANCE.....	7
3.	OVERVIEW OF THE COMMITTEE'S ACTIVITIES IN 2021.....	8
3.1	OVERSIGHT ACTIVITIES CARRIED OUT	8
3.2	THE COMMITTEE'S OVERSIGHT METHODS	8
3.3	THE COMMITTEE'S CONSIDERATION OF COMPLAINTS	8
3.4	SPECIAL REPORT TO THE STORTING	9
3.5	CONSULTATION SUBMISSION ON PST'S INTELLIGENCE MANDATE AND USE OF OPENLY AVAILABLE INFORMATION	9
3.6	CONSULTATION SUBMISSION ON PROPOSED AMENDMENTS TO THE POLICE DATABASES REGULATIONS ..	9
3.7	INPUT TO THE STORTING'S CONSIDERATION OF THE REPORT ON THE STORTING'S SUPERVISORY FUNCTIONS	10
3.8	EXTERNAL ACTIVITIES	10
4	THE NORWEGIAN POLICE SECURITY SERVICE (PST)	11
4.1	GENERAL INFORMATION ABOUT THE OVERSIGHT	11
4.2	PST'S REGISTRATION OF INDIVIDUALS.....	11
4.3	FOLLOW-UP OF PST'S SHARING OF INFORMATION WITH STATES WHERE THERE IS A RISK THAT HUMAN RIGHTS WILL NOT BE RESPECTED	11
4.4	FOLLOW-UP OF THE AIRLINE PASSENGERS CASE.....	11
4.5	TERRORIST SCREENING CENTER.....	12
4.6	ABOUT PST'S DISCLOSURE OF INFORMATION IN SECURITY CLEARANCE CASES.....	12
4.7	COMPLAINTS AGAINST PST	12
5	THE NORWEGIAN INTELLIGENCE SERVICE (NIS)	13
5.1	GENERAL INFORMATION ABOUT THE OVERSIGHT	13
5.2	FAILURE TO SUBMIT CASES THAT HAVE BEEN SUBMITTED TO THE MINISTRY OF DEFENCE.....	13
5.3	NEW INTELLIGENCE SERVICE ACT AND OVERSIGHT OF FACILITATED BULK COLLECTION	13
5.4	COMPLAINTS AGAINST THE NIS	14
6	THE NATIONAL SECURITY AUTHORITY (NSM)	15
6.1	GENERAL INFORMATION ABOUT THE OVERSIGHT	15
6.2	GROUND FOR DECISIONS IN SECURITY CLEARANCE CASES	15
6.3	THE SPECIALLY APPOINTED LAWYER ARRANGEMENT SET OUT IN THE SECURITY ACT	16
6.4	COMPLAINTS AGAINST NSM.....	16
6.5	CASE PROCESSING TIMES IN SECURITY CLEARANCE CASES.....	17
7	THE NORWEGIAN DEFENCE SECURITY DEPARTMENT (FSA).....	18
7.1	GENERAL INFORMATION ABOUT THE OVERSIGHT	18
7.2	SECURITY CLEARANCE OF NATIONAL SERVICE PERSONNEL	18
7.3	COMPLAINTS AGAINST FSA	18
7.4	CASE PROCESSING TIMES IN SECURITY CLEARANCE CASES.....	19
8	THE CIVIL SECURITY CLEARANCE AUTHORITY (SKM)	20
8.1	GENERAL INFORMATION ABOUT THE OVERSIGHT	20
8.2	COMPLAINT AGAINST THE SECURITY CLEARANCE AUTHORITY'S REFUSAL TO CONSENT TO AUTHORISATION	20
8.3	CASE PROCESSING TIMES IN SECURITY CLEARANCE CASES IN SKM	21
9	OVERSIGHT OF OTHER EOS SERVICES.....	22
9.1	GENERAL INFORMATION ABOUT THE OVERSIGHT	22

9.2	INSPECTION OF THE ARMY INTELLIGENCE BATTALION	22
9.3	INSPECTION OF THE NORWEGIAN ARMY SPECIAL FORCES COMMAND	22
9.4	THE STORTING'S ADMINISTRATION AND THE PRESIDUM OF THE STORTING AS SECURITY CLEARANCE AUTHORITIES	22
10	APPENDICES.....	23
	APPENDIX 1 – MEETINGS, VISITS, LECTURES AND PARTICIPATION IN CONFERENCES ETC.	23
	APPENDIX 2 – SPECIAL REPORT TO THE STORTING ON CLASSIFIED INFORMATION IN THE FRODE BERG CASE.	24
	APPENDIX 3 – CONSULTATION SUBMISSION ON PST'S INTELLIGENCE MANDATE AND USE OF OPENLY AVAILABLE INFORMATION.....	25
	APPENDIX 4 – CONSULTATION SUBMISSION ON THE PROPOSED AMENDMENTS TO THE POLICE DATABASES REGULATIONS.....	30
	APPENDIX 5 – INPUT TO THE STORTING'S CONSIDERATION OF THE HARBERG COMMITTEE'S REPORT	32
	APPENDIX 6 – ACT RELATING TO OVERSIGHT OF INTELLIGENCE, SURVEILLANCE AND SECURITY SERVICES.....	34

1. The Committee's remit and composition

The EOS Committee is a permanent, Storting-appointed oversight body whose task it is to oversee all Norwegian entities that engage in intelligence, surveillance and security activities (EOS services). Only EOS services carried out by, under the control of or initiated by the public administration are subject to oversight by the EOS Committee.¹

Pursuant to the Oversight Act² Section 2 first paragraph, the purpose of the oversight is:

- 1) to ascertain whether the rights of any person are violated and to prevent such violations, 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 unduly harm the interests of society, and
- 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 not seek more extensive access to classified information than warranted by the oversight purposes,³ and shall insofar as possible show consideration for the protection of sources and safeguarding of information received from abroad. Subsequent oversight is practised in relation to individual cases and operations, but the Committee is entitled to be informed about and express an opinion on the services' current activities. The

Committee may not instruct the EOS services it oversees or be used by them for consultations. The oversight shall cause as little inconvenience as possible to the services' operational activities. The Committee shall show consideration for national security and relations with foreign powers in its oversight activities.⁴

The Committee conducts reviews of legality. This means that it does not review the services' effectiveness, how they prioritise their resources etc.

The 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.⁵ No deputy members are appointed.

The Committee is independent of both the Storting and the Government. The Government cannot issue instructions to the Committee. The Storting may, however, in plenary decisions order the Committee to undertake specified investigations within the oversight remit of the Committee.

Committee members cannot also be members of the Storting, nor can they previously have worked in the EOS services. The committee members and secretariat employees must have top level security

¹ References to the Oversight Act are found in the Act relating to National Security (the Security Act) Section 11-1, the Act relating to the Norwegian Intelligence Service (the Intelligence Service Act) Section 2-6, and the Act relating to the Processing of Data by the Police and the Prosecuting Authority (the Police Databases Act) Section 68.

² Act No 7 of 3 February 1995 relating to the Oversight of Intelligence, Surveillance and Security Services (the Oversight Act). The Act was most recently amended in June 2020, when the Security Act was made applicable to the EOS Committee, with certain exemptions.

³ Cf. the Oversight Act Section 8 third paragraph. It is stated in the Oversight Act Section 8 fourth paragraph that the Committee can make binding decisions regarding access and the scope and extent of the 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. In 1999, the Storting adopted a plenary decision for a special procedure to apply in connection with disputes about access to the Norwegian Intelligence Service documents. The decision did not lead to any amendments being made to the Act or Directive governing the

Committee's oversight activities, 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. The Storting's 1999 decision was based on the particular sensitivity associated with some of the Norwegian Intelligence Service's sources, the identity of persons with roles in occupation preparedness and particularly sensitive information received from foreign partners. In 2013, the EOS Committee asked the Storting to clarify whether the Committee's right of inspection as enshrined in the Act and Directive shall also apply in full in relation to the Norwegian Intelligence Service, 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, see Document 16 (2015–2016). When the Evaluation Committee's report was considered in 2017, the limitation on access to 'particularly sensitive information' was upheld without the wording of the Act being amended.

⁴ Cf. the Oversight Act Section 2.

⁵ Cf. the Oversight Act Section 3.

clearance and authorisation, both nationally and pursuant to treaties to which Norway is a signatory.⁶ 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 for 2021:

The Committee during the first six months of 2021:

Svein Grønnern, Oslo, chair	13 June 1996	–	30 June 2021
Astri Aas-Hansen, Asker, deputy chair	1 July 2019	–	30 June 2024
Øyvind Vaksdal, Karmøy	1 January 2014	–	30 June 2021
Eldfrid Øfsti Øvstedal, Trondheim	1 July 2016	–	30 June 2021
Magnhild Meltveit Kleppa, Hjelmeland	1 July 2019	–	30 June 2024
Erling Johannes Husabø, Bergen	1 July 2019	–	30 June 2024
Camilla Bakken Øvald, Oslo	1 July 2019	–	30 June 2024

The Committee during the last six months of 2021:

Astri Aas-Hansen, Asker, chair	1 July 2019	–	30 June 2024
Kristin Krohn Devold, Oslo, deputy chair	1 July 2021	–	30 June 2025
Magnhild Meltveit Kleppa, Hjelmeland	1 July 2019	–	30 June 2024
Erling Johannes Husabø, Bergen	1 July 2019	–	30 June 2024
Camilla Bakken Øvald, Oslo	1 July 2019	–	30 June 2024
Jan Arild Ellingsen, Saltdal	1 July 2021	–	30 June 2025
Olav Lysne, Bærum	1 July 2021	–	30 June 2025

Of the seven board members, five have political backgrounds from different parties. The other two have professional backgrounds from the fields of law and technology.

⁶ Cf. the Oversight Act Section 11 second paragraph.

2. Key figures and governance

The Committee's expenses amounted to NOK 33,612,000 in 2021. The total budget, including transferred funds, amounted to NOK 35,900,000. The Committee has applied for permission to transfer NOK 1,730,000 in unused funds to its budget for 2022.

In 2019, the Committee was allocated NOK 29,000,000 to refurbish its new premises. The project was completed in accordance with the budget. The costs amounted to NOK 28,922,000.

The workload of the chair of the Committee corresponds to about 30 per cent of a full-time position, while the office of committee member is equivalent to about 20 per cent of a full-time position.

The Committee is supported by a secretariat. At year end 2021, the Committee Secretariat consisted of 19 full-time employees: the head of the secretariat, a legal unit with a staff of seven, a technology unit with a staff of six and an administrative unit with a staff of five.⁷ Three positions were vacant.

It will be necessary to add to the secretariat staff in the years ahead due to, among other things, the introduction of facilitated bulk collection as a new method for the Norwegian Intelligence Service. The Storting has requested the Presidium of the Storting to ensure that the EOS Committee receives sufficient resources in the annual budget allocations.⁸ In its budget proposal for 2022, the Committee informed the Presidium of the Storting that it will need 30 secretariat employees in 2025.

Sickness absence in the Secretariat was 4.1 per cent in 2021, compared with 4.8 per cent in 2020.

The Auditor General is the EOS Committee's external auditor.

⁷ An office manager, a head of security, a communications adviser and two employees with responsibility for financial matters, HR, archive and office functions.

⁸ Resolution 677, cf. Enactment of Bill 134 (2019–2020).

3. Overview of the Committee's activities in 2021

3.1 Oversight activities carried out

In 2021, the Committee conducted 18 inspections. The Police Security Service was inspected six times, the Norwegian Intelligence Service (NIS) six times, the National Security Authority (NSM) twice⁹ and the Norwegian Defence Security Department twice. The Army Intelligence Battalion, the Norwegian Special Operation Forces and the Civil Security Clearance Authority were all inspected once.

In 2021, the Committee held nine internal full-day meetings, in addition to internal working meetings on site in connection with inspections. During the internal meetings, the Committee discusses planned and completed inspections, complaints and cases raised on the Committee's own initiative, reports to the Storting and administrative matters.

The Committee raised 13 cases with the services on its own initiative in 2021, compared with 16 in 2020. The Committee concluded 16 cases raised on its own initiative in 2021, compared with 10 cases in 2020.

The Committee investigates complaints from individuals and organisations. In 2021, the Committee received 25¹⁰ complaints against the EOS services, compared with 29 complaints in 2020. The Committee concluded 26 complaints in 2021, compared with 30 complaints in 2020.¹¹

3.2 The Committee's oversight methods

The Committee's inspections consist of a briefing part and an inspection part. The topics of the briefings are mostly selected by the Committee, but the services are also

asked to brief the Committee on any matters they deem to be relevant to the Committee's oversight, including non-conformities that they themselves have identified.

The Committee is briefed about the service's ongoing activities, national and international cooperation, and cases that have given rise to public debate. The Committee asks verbal questions during the briefings and sends written questions afterwards.

During the inspection part, the Committee conducts searches directly in the service's computer systems. The services are not informed about what the Committee search for. This means that the inspections contain considerable unannounced elements. The goal is to conduct the most qualified spot check-based oversight possible. The Secretariat makes thorough preparations in the services' computer systems which enable the Committee to conduct targeted inspections.

The Committee raises cases on its own initiative based on findings made during its inspections.¹² Such cases are also raised based on notifications received or public attention. Documents from the service in question are reviewed in order to shed light on the matter. The services' employees can also be summoned for interviews. The service must always be given the opportunity to state its opinion on the issues raised in the case before the Committee submits its statement.

3.3 The Committee's consideration of complaints

Complaints that fall within the Committee's oversight area are investigated in the service or services that the complaint concerns. The

⁹ One of the inspections of NSM took place with only four committee members present.

¹⁰ Several complaints concern more than one of the services.

¹¹ These figures also include a small number of complaints that have been dismissed or withdrawn.

¹² Cf. the Oversight Act Section 5 third paragraph.

Committee has a low threshold for considering complaints. An increasing proportion of the complaints are complex. The Committee has spent more resources on considering complaints in 2021 than before.

The Committee's statements to complainants shall be unclassified. It is classified information that a person has *not* been registered by the service.¹³ In such cases, the Committee will inform the complainant that the complaint has been investigated and that the Committee has not found that the service has broken the law or acted in a manner that warrants criticism. The complainant is *not* informed that he or she has not been registered by the service.

It is also classified information that a person has been subjected to *lawful* surveillance activities by the service. In such cases, the Committee will inform the complainant that the complaint has been investigated and that the Committee has not found that the service has broken the law or acted in a manner that warrants criticism. The complainant is *not* informed that he or she has been subjected to *lawful* surveillance.

Only in cases where the Committee's investigation shows that the complainant's rights have been violated can the Committee confirm to the complainant that he or she has been registered by the service – in that the Oversight Act allows the Committee to state that it found grounds for criticism.

If the Committee is of the opinion that a complainant should be given a more detailed explanation, it can propose this to the service in question or the responsible ministry. The service's decision regarding classification of information is binding on the Committee.¹⁴ The Committee is therefore prevented from informing the complainant about the basis for criticism without the consent of the service or the responsible ministry.

¹³ The Oversight Act Section 15 first paragraph second sentence reads as follows: 'Information concerning whether or not a person has been subjected to surveillance activities shall be regarded as classified unless otherwise decided.'

¹⁴ Cf. the Oversight Act Section 11 final paragraph final sentence.

¹⁵ Document 7:2 (2020–2021).

3.4 Special report to the Storting

On 25 February 2021, the Committee submitted a special report to the Storting concerning the Frode Berg case 'to notify the Storting that consideration for the Storting's supervision of the administration dictates that the Storting should familiarise itself with classified information, cf. the Oversight Act Section 17 second paragraph.'¹⁵ At the Storting's request, the Committee submitted its classified final report and an abbreviated version. The special report is enclosed as Appendix 2.

3.5 Consultation submission on PST's intelligence mandate and use of openly available information

In 2021, the Ministry of Justice and Public Security distributed for consultation a proposal to enshrine PST's intelligence mandate in law. The Ministry also proposed giving the service legal authority to collect, analyse and store large quantities of openly available information for a period of 15 years. The Committee stated that from an oversight perspective, a more detailed assessment of several factors would be desirable.

The EOS Committee's consultation submission dated 17 December 2021 is enclosed as Appendix 3.

3.6 Consultation submission on proposed amendments to the Police Databases Regulations

In 2021, the Ministry of Justice and Public Security distributed for consultation a proposal to amend the Police Databases Regulations' provisions on processing of information by PST. In its consultation submission, the Committee pointed out the importance of written grounds as a basis for real and effective subsequent oversight of PST.

The EOS Committee's consultation submission dated 11 May 2021 is enclosed as Appendix 4.

3.7 Input to the Storting's consideration of the report on the Storting's supervisory functions

The committee appointed to assess the Storting's supervisory function submitted its report in 2021.¹⁶ The EOS Committee submitted some comments on matters discussed in the report that directly touched on the EOS Committee's activities.

The EOS Committee's letter of 24 March 2021 to the Storting's Standing Committee

on Scrutiny and Constitutional Affairs is enclosed as Appendix 5.

3.8 External activities

In 2021, the Committee met with Minister of Defence Frank Bakke-Jensen (Con.), Minister of Justice and Public Security Monica Mæland (Con.) and Minister of Justice and Public Security Emilie Enger Mehl (Centre Party). At these meetings, the Committee described its oversight of the EOS services.

The Committee has also attended several external events, see Appendix 1.

¹⁶ Document 21 (2020-2021) *Rapport fra utvalget til å utrede Stortingets kontrollfunksjon*.

4 The Norwegian Police Security Service (PST)

4.1 General information about the oversight

In 2021, the Committee conducted six inspections of the Norwegian Police Security Service (PST). Four inspections were conducted of the PST headquarters (DSE) in Oslo. The Committee also inspected the PST entities in the Trøndelag and Southeastern police districts.

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

- The service's collection and processing of personal data
- The service's new and concluded prevention cases, averting investigation cases and investigation cases
- The service's use of covert coercive measures (for example telephone and audio surveillance, equipment interference and covert searches) and handling of sources
- The service's exchange of information with foreign and domestic partners

4.2 PST's registration of individuals

In its oversight of PST's registrations for preventive purposes, the Committee focuses on checking that the requirements regarding necessity, relevance and specification of purpose are met. One important focus is the strict necessity requirement that applies to the processing of special categories of personal data, for example a person's political or religious beliefs, cf. the Police Databases Act Section 7.

In 2021, the Committee has asked PST about the service's registration of six persons for preventive purposes. In five cases, PST replied that there was no grounds for processing information about the person in question and that the information would be deleted. The Committee agreed

with PST's assessment and criticised the service for having registered these people without grounds. In one of the five cases, the Committee noted that it was particularly unfortunate that the lacking grounds for registration had not been identified in the mandatory five-year review. It further strengthened the Committee's criticism that the registration in question contained information about the person's political beliefs.

In the sixth case, the Committee criticised PST and stated that the registration should have been deleted. However, PST maintained that there were grounds for registering this person. Consequently, the information has not been deleted.

4.3 Follow-up of PST's sharing of information with states where there is a risk that human rights will not be respected

The annual report for 2020¹⁷ discussed the EOS Committee's criticism of PST's exchange of information about a Norwegian citizen with a service in a country where there is a risk that the authorities will not respect human rights. The Committee stated that PST's assessment of the risk of human rights violations associated with disclosing this information was incomplete.

In an inspection of PST in 2021, the Committee followed up the matter by examining internal procedures and disclosures in general.

The Committee found no basis for further follow-up.

4.4 Follow-up of the airline passengers case

In a special report¹⁸ submitted in 2019, the Committee criticised PST for having

¹⁷ Document 7:1 (2020–2021), Section 4.2

¹⁸ Document 7:2 (2019–2020) Special report to the Storting on PST's unlawful collection and storage of information about airline passengers.

collected and stored a large quantity of information about Norwegians' air travel. There was no legal basis for this collection, and it was thus unlawful. PST has stated that the airline passenger information has been deleted.

Following the submission of the special report, PST has established a new entity with responsibility for the service's internal control and risk management.

The Committee is satisfied with PST's follow-up and has concluded the matter.

4.5 Terrorist Screening Center

The Committee has mentioned in its annual reports for 2013, 2014, 2016 and 2017 that information about Norwegians was registered in a database belonging to the FBI (Terrorist Screening Center).

The Committee has received a statement from the Ministry of Justice and Public Security regarding what information is entered into the database, who enters the information, how the data are used, possibilities for correction and deletion of data, and the consequences of being registered.

The Ministry's briefing did not give grounds for follow-up, and the Committee has concluded the matter.

4.6 About PST's disclosure of information in security clearance cases

In its annual report for 2018,¹⁹ the Committee wrote that PST's practice for disclosure of information to security clearance authorities did not comply with the statutory and regulatory requirements. The Committee criticised PST's practice of

disclosing personal data verbally. The Committee emphasised how important it is for PST to make clear any uncertainty associated with the information disclosed to the security clearance authorities.

NSM is the expert authority responsible for security clearance in Norway. During an inspection in 2021, NSM informed the Committee that the Directorate no longer sees any challenges associated with exchange of information with PST in security clearance cases.

4.7 Complaints against PST

The Committee received 17 complaints against PST in 2021, compared with 19 complaints in 2020. Some of these complaints were directed against more than one of the EOS services. The Committee concluded 12 complaints against PST in 2021. Two complaints resulted in criticism of PST, while ten cases were concluded without criticism.

In one complaint case, PST rejected the Committee's proposal to give the complainant a more detailed explanation of the grounds for the Committee's criticism, cf. the Oversight Act Section 15. The Committee informed the complainant that it had expressed criticism against the service.

In the other complaint case, PST accepted the Committee's proposal to give the complainant a more detailed explanation of the grounds for the criticism. The Committee criticised PST for having processed information about the complainant for longer than required for the purpose of the processing. The information about the complainant has been deleted.

¹⁹ Document 7:1 (2018–2019), Section 5.2.

5 The Norwegian Intelligence Service (NIS)

5.1 General information about the oversight

The Committee conducted four inspections of the Norwegian Intelligence Service (NIS) headquarters in 2021, in addition to one inspection of a local station, the Norwegian Armed Forces' station on Andøya. The station on Andøya collects, analyses and reports maritime activity in the High North.

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

- The NIS's use of collection methods that could entail interference in relation to individuals²⁰
- The service's processing of information
- The service's exchange of information with domestic and foreign partners
- Cases that have been submitted to the Ministry of Defence²¹ and internal approval cases²²
- National control of the NIS's stations, equipment, methods and information collection

The Committee's right of access does not extend to information defined as particularly sensitive information²³ by the NIS. The Committee is regularly informed about the scope of information that falls within this category. The information is made available to the Committee once it is no longer defined as being particularly sensitive.²⁴

5.2 Failure to submit cases that have been submitted to the Ministry of Defence

The Committee learnt that, during the period 2011–2020, not all cases that the NIS had

submitted to the Ministry of Defence pursuant to the Intelligence Service Act Section 2-5 had been submitted to the Committee. The service has apologised for this failure, which was due to a procedural failure.

The EOS Committee has emphasised to the service that it expects to be informed of all cases and operations submitted to the Ministry of Defence for approval.

5.3 New Intelligence Service Act and oversight of facilitated bulk collection

The Intelligence Service Act chapters 7 and 8 came into force 1 January 2022, with the exception of Section 7-3. A new oversight responsibility was thereby added to the Committee's remit. It follows from Section 7-11 of the Act that the Committee is to carry out continuous oversight of the method facilitated bulk collection. Facilitated bulk collection means that the NIS can collect electronic communication transmitted across the Norwegian border. If the EOS Committee believes that the NIS uses this method in an unlawful manner, the Committee can submit a petition to the district court requesting that the unlawful activities cease.

This continuous oversight requires more extensive oversight methods. The Committee needs the service to allocate sufficient resources to establishing and operating oversight functionality in their systems. The Committee started developing an oversight concept for facilitated bulk collection in 2021.

²⁰ The Intelligence Service Act Chapter 6.

²¹ Pursuant to the Intelligence Service Act Section 2-5, the Ministry's approval is required in cases concerning a) the establishment of collaboration and agreements with foreign services or international organisations, b) the launching of special intelligence operations that could raise political issues, c) other cases of particular importance.

²² Internal approval cases can concern permission to share information about Norwegian persons with foreign partners or to monitor Norwegian persons' communication when the persons are abroad.

²³ 1. The identity of the human intelligence sources of the NIS and its foreign partners 2. The identity of foreign partners' specially protected civil servants 3. Persons with roles in and operational plans for occupation preparedness 4. The NIS's and/or foreign partners' particularly sensitive intelligence operations abroad which, were they 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.

²⁴ Read more in section 5.5 of the Committee's annual report for 2020.

5.4 Complaints against the NIS

The Committee received ten complaints against the NIS in 2021, compared with eight complaints in 2020. Some of these complaints were against more than one of the EOS services.

The Committee concluded eight complaints against the NIS in 2021. None of the concluded cases resulted in criticism of the NIS.

6 The National Security Authority (NSM)

6.1 General information about the oversight

In 2021, the Committee conducted two inspections of the National Security Authority (NSM). One of the inspections focused on NSM's processing of security clearance cases. The other inspection was of the Norwegian National Cyber Security Centre (NCSC).²⁵

During its inspections of NSM, 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 case processing times in security clearance cases
- NSM's cooperation with other EOS services
- NSM's processing of personal data
- NSM's technical capabilities

6.2 Grounds for decisions in security clearance cases

Persons who are denied security clearance shall be informed about the outcome and the grounds for the decision. The Security Act lists certain circumstances that should not be included in the grounds.²⁶ The security clearance authority shall prepare internal grounds that include all relevant factors.

The Committee has noted that the security clearance authorities' views differ when it comes to the relationship between the grounds given to the vetted person and the security clearance authority's internal grounds.

In response to a question from the Committee, the Ministry of Justice and

Public Security answered that the security clearance authority can only omit those parts of the grounds that fall within the scope of the exemptions in the Security Act Section 8-13 second paragraph. The Ministry also stated that 'the grounds are normally (...) limited to describing the gist of the information and circumstances that the security clearance authority has given weight to in the overall assessment that forms the basis for the case'. The Committee based its further work on the Ministry's view.

The Committee pointed out to the Ministry that the vetted person is often not informed that information has been omitted from the grounds given as envisaged in the Security Act. Moreover, the internal grounds contain no written assessments of what information should be omitted from the grounds disclosed to the person in question. The absence of such assessments makes it difficult for the Committee to review the reasons why the security clearance authority has not communicated the information to the vetted person. The absence of information can also give the person the impression that the case processing has been more general and superficial than is actually the case. The Committee informed the Ministry that it expects the security clearance authorities to inform the vetted person when the internal grounds contain information that is omitted pursuant to the Security Act Section 8-13.

The Committee asked the Ministry of Justice and Public Security to ensure that the security clearance authorities interpret and practise the legislation in a uniform manner. The Ministry has asked NSM to take steps to ensure a more uniform practice.

²⁵ The function of NCSC is to protect fundamental national functions, the public administration and business and industry against serious cyber attacks. To perform its tasks, NCSC can process specified personal data, cf. the Security Act Section 2-4.

²⁶ The Security Act Section 8-13. For example, the grounds given shall not include information which may reveal circumstances which are relevant to national security interests.

6.3 The specially appointed lawyer arrangement set out in the Security Act

Persons are entitled to the assistance of a specially appointed lawyer if information has been omitted from the grounds for a decision in a security clearance case pursuant to the Security Act Section 8-13.²⁷ The purpose of this arrangement is to compensate for the disadvantages of not receiving more detailed grounds. It was established in 2006.

The Committee's investigations showed that the arrangement has not been used for the past ten years. The Committee has stated to the Ministry of Justice and Public Security that assistance from a specially appointed lawyer might have been relevant in a number of cases.

The procedure for making use of a specially appointed lawyer is complicated and time-consuming. The Committee noted that practices differ between the security clearance authorities when it comes to providing information about the mechanism. The Committee asked the Ministry to take steps to ensure that the lawyer arrangement functions as intended.

The Ministry has responded that it largely agrees with the Committee, and that it has been pointed out to NSM that the vetted person should be informed of the right to a lawyer in cases where it is relevant. The Ministry will consider initiating work to take a closer look at this arrangement.

6.4 Complaints against NSM

The Committee received nine complaints against NSM in 2021, compared with twelve complaints in 2020. Some of these complaints were against more than one of the services. The Committee concluded eleven complaints in 2021. Two of the cases resulted in criticism.

In one complaint case, NSM was criticised for letting a security clearance case sit for more than six months without case processing steps being taken. The time that elapsed was due solely to the case being 'in the queue'.

When considering the complaint, the Committee also considered NSM's case processing times in other cases. NSM's goal for 2021 was that cases considered by the directorate as an appellate body should be processed within 90 days. During the first four months of 2021, the average case processing time for such cases was more than twice of that goal. The Committee criticised NSM for long case processing times in cases where NSM considers complaints as the appellate body. The Committee expects NSM to take steps to reduce its case processing times.

In the other complaint case, NSM was criticised for having taken more than four months to process a case about access to information.

²⁷ The Security Act Section 8-15.

6.5 Case processing times in security clearance cases

Below is a table of case processing times for 2021 as provided by NSM:²⁸

	Average case processing time overall	Average case processing time, positive decisions ²⁹	Average case processing time, negative decisions
Request for access to information	91 days ³⁰ (2 cases)		
Request for security clearance	87 days (105 cases)	74 days (98 cases)	277 days (7 cases)
First-tier appeals	No cases		
Second-tier appeals	289 days (31 cases)	389 days (3 cases)	278 days (28 cases) ³¹

The Committee is concerned about the fact that NSM's case processing times have increased in nearly all areas in 2021 compared with 2020. The Committee expects NSM to take steps to reduce its case processing times.

²⁸ The statistics are based on the date on which the request was received by the security clearance authority.

²⁹ In the statistics for SKM and NSM, figures for appeals granted in part are included under 'positive decisions', while for FSA, such appeals are included under 'negative decisions'.

³⁰ NSM also considered appeals concerning requests for access to information for which the directorate was the appellate body. The case processing time for such cases was 135 days.

³¹ The average case processing time for appeal cases that were dropped or dismissed was 134 days based on 15 cases. The 28 cases included in the table concern appeals that were not granted.

7 The Norwegian Defence Security Department (FSA)

7.1 General information about the oversight

The Committee conducted two inspections of the Norwegian Defence Security Department (FSA) in 2021. One of the inspections focused on FSA's processing of security clearance cases. The other one focused on FSA's operational security services.

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

- FSA's processing of cases where security clearance has been denied, reduced or suspended by the security clearance authority
- FSA's case processing times in security clearance cases
- FSA's operational security activities
- FSA's processing of personal data as part of its protective security services
- FSA's cooperation with other EOS services

7.2 Security clearance of national service personnel

Security clearance at SECRET/NATO SECRET level is required for all positions that personnel may serve in during their national service.³²

In 2021, the Committee received a notification of concern regarding the security clearance process for soldiers in national service. The notification was seen in conjunction with several enquiries received by the Committee from persons who received negative decisions in security clearance cases during their national service.

FSA informed the Committee that the Armed Forces endeavour at an early stage to identify persons whose connections to other states could cause the processing of their security clearance case to take longer than usual. In 2020, the Norwegian Armed Forces HR and Conscription Centre (FPVS) introduced a procedure whereby persons with a known connection to certain countries submit their personal data form earlier than other personnel summoned for examination for military service. The purpose of this is to gain time in the case processing. If the security clearance case has not been decided two months before the intake date, the person in question will not be included in that intake. This has reduced the number of persons who receive a negative security clearance decision after having started their national service.

7.3 Complaints against FSA

The Committee received six complaints against FSA in 2021, the same number as in 2020. Some of these complaints were against more than one of the services. Six complaints against FSA were concluded in 2021. None of the concluded cases resulted in criticism of FSA.

³² The Norwegian Armed Forces HR and Conscription Centre (FPVS) has informed the Committee that the security clearance level for all positions in the Armed Forces would be reviewed by the end of 2021.

7.4 Case processing times in security clearance cases

Below is a table of case processing times for 2021 as provided by FSA:³³

	Average case processing time overall	Average case processing time, positive decisions ³⁴	Average case processing time, negative decisions
Request for access to information	9 days (28 cases)		
Requests for security clearance	42 days (21,524 cases)	38 days (21,131 cases)	223 days (393 cases ³⁵)
First-tier appeals	176 days (59 cases)	187 days (13 cases)	172 days (46 cases ³⁶)

Overall, the average case processing time has been reduced from 2020 to 2021.

³³ The statistics are based on the date on which the request was received by the security clearance authority.

³⁴ In the statistics for SKM and NSM, figures for appeals granted in part are included under 'positive decisions', while for FSA, such appeals are included under 'negative decisions'.

³⁵ In 233 of these cases the decision was NO CLEARANCE, while in the remaining cases, clearance was granted subject to conditions, for a lower level or shorter time than requested, or with a combination of such limitations.

³⁶ This figure includes 10 decisions that were granted in part.

8 The Civil Security Clearance Authority (SKM)

8.1 General information about the oversight

The Committee carried out one inspection of the Civil Security Clearance Authority (SKM) in 2021. SKM briefed the Committee about its internal control, case processing times and experience with conditional security clearance.³⁷

The Committee received and concluded its consideration of one complaint against SKM in 2021. The complaint did not give grounds for criticism, but did result in further investigations as described in the section below.

8.2 Complaint against the security clearance authority's refusal to consent to authorisation

The Committee received a complaint from a person who holds dual citizenship of Norway and a country that PST deems to represent a great security risk to Norway. The employer could not authorise³⁸ the person for the RESTRICTED security classification without the consent of the security clearance

authority.³⁹ SKM refused to consent to the authorisation. The person was not given grounds for the rejection and was not given right of appeal.

The Committee stated to the Ministry of Justice and Public Security that the case illustrates shortcomings in the rules concerning authorisation of foreign nationals. The Committee urged the Ministry to 'establish rules for grounds, access to information and appeals in authorisation cases where the consent of the security clearance authority is required'.

The Ministry of Justice and Public Security has replied that it shares the Committee's views. In its letter, the Ministry wrote that it will 'shortly consider initiating regulatory collaboration for the purpose of adopting provisions on right of appeal in cases where the security clearance authority does not consent to authorisation'.

After reconsidering the case, SKM has consented to the complainant being authorised.

³⁷ A security clearance authority may grant a person security clearance subject to specific conditions, for example that the clearance is limited to a specific position or a shorter period than usual.

³⁸ Decision about whether to grant a person access to information with a specified security classification.

³⁹ The Security of Undertakings Regulations Section 70 second paragraph.

8.3 Case processing times in security clearance cases in SKM

Below is a table of case processing times for 2021 as provided by SKM:⁴⁰

	Average case processing time overall	Average case processing time, positive decisions ⁴¹	Average case processing time, negative decisions
Request for access to information ⁴²	8 days (44 cases)		
Request for security clearance ⁴³	53 days (5,986 cases)	43 days (5,734 cases)	283 days (252 cases)
First-tier appeals	182 days (54 cases)	350 days (9 cases)	148 days (45 cases)

The Committee notes that the average case processing time has increased for negative security clearance decisions and increased even more for appeal cases, particularly for positive decisions.

⁴⁰ The statistics are based on the date on which the request was received by the security clearance authority.

⁴¹ In the statistics for SKM and NSM, figures for appeals granted in part are included under 'positive decisions', while for FSA, such appeals are included under 'negative decisions'. No first-tier appeals were granted in full by SKM in 2021.

⁴² Average case processing time for appeal cases concerning access to information was 14 days in 2021.

⁴³ SKM has also provided information about the average case processing time for incoming information in security clearance cases. In 2021, it averaged 160 days.

9 Oversight of other EOS services

9.1 General information about the oversight

The Committee oversees EOS services regardless of which part of the public administration the services are carried out by.⁴⁴ The oversight area is defined by function rather than being limited to certain organisations.

The Committee shall carry out one inspection per year of the Army Intelligence Battalion and one inspection per year of the Norwegian Special Operation Forces.⁴⁵

The Committee has received three complaints against different organisational entities that engage in EOS services in 2021. Five complaints against other intelligence, surveillance or security services were concluded in 2021, all without criticism.

9.2 Inspection of the Army Intelligence Battalion

The main topic of the Committee's inspection of the Army Intelligence Battalion (Ebn) at Setermoen in Troms was the battalion's cooperation with the Norwegian Intelligence Service.⁴⁶ The Committee was also briefed about Ebn's ongoing activities since the previous inspection. The Committee inspected Ebn's computer systems and selected documents. The inspection did not give grounds for follow-up.

Following its inspection of Ebn in autumn 2020, the Committee asked Ebn about the battalion's contracts with actors⁴⁷ for participation in exercises. When concluding the case in 2021, the Committee stated that the Personal Data Act Section 16 first paragraph letter a), cf. the Freedom of

Information Act Section 21, does not provide a legal basis for a general exemption from the actors' right of access to personal data about them being processed.

9.3 Inspection of the Norwegian Army Special Forces Command

During the inspection of the Norwegian Special Forces Command (FSK) at Rena base in Hedmark, the Committee was briefed about FSK's key activities, exercises, capacities and cooperation. The briefing also covered how human rights are safeguarded when FSK serves abroad.

The inspection did not give grounds for follow-up.

9.4 The Storting's administration and the Presidium of the Storting as security clearance authorities

It follows from the Security Act Section 11-1 that 'protective security work pursuant to the act is subject to the control and supervision' of the EOS Committee. Section 2 of the provisions for the application of the Security Act in relation to the Storting's administration states that Section 11-1 of the Security Act does not apply to the Storting's administration. The Storting's administration and the Presidium are thus exempt from the EOS Committee's oversight of security clearance cases.

Based on the above, the EOS Committee rejects complaints against security clearance decisions made by the Storting in its capacity as security clearance authority.

⁴⁴ The Oversight Act Section 1 first paragraph.

⁴⁵ Cf. the Oversight Act Section 7.

⁴⁶ See the EOS Committee's annual report for 2019, section 10.2, for more information about this cooperation.

⁴⁷ Civilians and/or former employees used as actors for training purposes and exercises.

10 Appendices

Appendix 1 – Meetings, visits, lectures and participation in conferences etc.

Meeting with the minister of defence

In January, the Committee met with Minister Frank Bakke-Jensen (Con.). At this meeting, the Committee described its oversight of the EOS services that fall within the minister of defence's area of responsibility.

Meetings with ministers of justice and public security

In 2021, the Committee met with Minister Monica Mæland (Con.) in February and Minister Emilie Enger Mehl (Centre Party) in December. At both these meetings, the Committee described its oversight of the EOS services that fall within the minister of justice and public security's area of responsibility.

Meeting with Lithuanian members of parliament and authorities

Committee chair Grønnern and two secretariat employees had a digital meeting with representatives of the Lithuanian parliament and authorities. Lithuania may become the first country in Eastern Europe to establish a dedicated external oversight body for its EOS services. The purpose of the meeting with the EOS Committee was to gather information in connection with the process of putting such an oversight body in place.

Participation in debate during Arendalsuka

In August, committee chair Aas-Hansen gave a talk at an event hosted by Simula. The topic was 'Who is listening to our secrets in computer networks?'

Oversight conference in Rome

In October, a committee member and a secretariat employee attended the third European Intelligence Oversight Conference, which brought together representatives of the oversight bodies of 14 countries in Europe. The conference's main topic were the judgments by the European Court of Human Rights in Strasbourg

concerning the bulk collection regimes of the UK and Sweden and their oversight.

Lecture for students at the Norwegian Defence University College

Committee chair Aas-Hansen and another member of the committee each gave a lecture on the EOS Committee for groups of students at the Norwegian Defence University College in November.

Lectures for law students at the University of Oslo

The Secretariat took part in the career day for law students in Oslo in February. The head of the secretariat gave a lecture on the activities of the EOS Committee. The head of the secretariat also gave a lecture for law students in Oslo in September.

Meeting with other European oversight bodies

The collaboration group Intelligence Oversight Working Group (IOWG) held a digital meeting in September. The Secretariat met with representatives of the oversight bodies of the UK, Denmark, the Netherlands, Belgium and Switzerland.

Meeting with the Swedish oversight body SIUN

In November, the head of the Secretariat's technology unit met representatives of the Swedish inspection authority for military intelligence activities (*Statens inspektion för försvarsunderrättelsesverksamheten*, abbreviated SIUN) in Stockholm.

Meeting with Canadian oversight body

In November, secretariat employees had a digital meeting with a legal adviser from the Canadian oversight body National Security and Intelligence Review Agency (NSIRA).

Appendix 2 – Special report to the Storting on classified information in the Frode Berg case

Special report to the Storting on classified information (Document 7:2 2020–2021)

To the Storting

The EOS Committee is the Storting's oversight body for the secret services. Our function is to oversee the intelligence, surveillance and security services. The EOS Committee has investigated the Frode Berg case on its own initiative. The Committee submitted its concluding statement in the case on 14 December 2020.

The Committee shall report to the Storting on its activities, and the reports shall be unclassified.

The Committee has on several occasions asked the public administration whether information in its statement can be declassified or given a lower security classification, including whether the Committee's conclusions can be communicated to the Storting unclassified. The public administration has decided that all the information is classified, including whether criticism has been expressed. In cases of doubt regarding the classification of information, the administration's decision is binding on the Committee, cf. the Oversight Act Section 11 third paragraph.

The Committee hereby submits a special report to the Storting to notify the Storting that consideration for the Storting's supervision of the administration dictates that the Storting should familiarise itself with classified information, cf. the Oversight Act Section 17 second paragraph. In this case, the Committee is of the opinion that the Storting should familiarise itself with the Committee's assessments and conclusions as described in the Committee's classified final report.

The Committee will submit the classified final report at the Storting's request.

Oslo, 25 February 2021



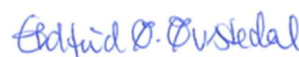
Svein Grønnern



Astri Aas-Hansen



Øyvind Vaksdal



Eldfrid Øfsti Øvstedal



Magnhild Meltveit Kleppa



Erling Johannes Husabø



Camilla Bakken Øvald

Henrik Magnusson



Appendix 3 – Consultation submission on PST's intelligence mandate and use of openly available information

The Ministry of Justice and Public Security
P.O. Box 8005 Dep.
NO-0030 OSLO

17 Dec. 2021

Our ref.: 2021/349-3

Your ref.: 21/4559 - NNO

Consultation submission from the EOS Committee – consultation on proposed amendments to the Police Act, the Police Databases Act and the Police Databases Regulations – PST's intelligence mandate and use of openly available information

1. Introduction

The EOS Committee refers to the Ministry of Justice and Public Security's consultation letter of 7 October 2021 on proposed amendments to the Police Act, the Police Databases Act and the Police Databases Regulations – PST's intelligence mandate and use of openly available information. The EOS Committee hereby submits its consultation statement.

It has been the EOS Committee's practice to have a high threshold for submitting consultation statements. It does not fall within the Committee's remit to have opinions about which tasks and surveillance methods the Storting as the legislative body and the Ministry at the regulatory level should assign to and permit the Police Security Service (PST) to use. The proposed amendments to the Police Act, the Police Databases Act and the Police Databases Regulations will impact the Committee's oversight activities, and this gives us reason to submit some comments.

The Committee has noted that the consultation paper consistently refers to the EOS Committee as a security mechanism. The EOS Committee is not intended to function as a guarantee that errors are not or cannot be made in the EOS services. Our oversight is based on spot checks and is not intended as a complete review of all surveillance activities carried out by PST. The Committee's external oversight is no replacement for management and supervision of PST by the government administration.

2. Comments to the proposal

2.1 On the relationship between police and intelligence activities

PST's role and responsibility is to prevent and investigate certain criminal offences, cf. the Police Act Section 17 b. In addition, the Police Act Section 17 c assigns special tasks to the PST headquarters (DSE), including to prepare threat assessments for use by the political authorities. The Ministry states that it is already 'assumed that PST is to engage in intelligence activities within its remit' and that this should be expressly stated in the Police Act.

Based on the above, a wording is proposed for PST's intelligence mandate in the Police Act Section 17 b new fourth paragraph. Consequently, it is proposed that PST be given independent legal authority to process information that is 'necessary for intelligence purposes', cf. proposed Section 64 third paragraph new sub-section 6.

The Committee would like to remark that there is a tradition for distinguishing between police and law enforcement functions on the one hand and intelligence functions on the other. The preparatory works to the new Intelligence Service Act described this distinction in principle as follows:

‘Unlike the police and prosecuting authority, which operate based on degrees of probability that someone has committed or is preparing to commit a criminal offence, the Intelligence Service considers whether the collection will meet the Norwegian authorities’ need for information. It is irrelevant whether anyone has committed or may commit a criminal offence, and the service has no duties related to prosecution. Considering these distinguishing features, the Ministry is of the opinion that the threshold for when the service can collect information, must be low.’⁴⁸

Since PST also has important prevention and investigation duties, it is difficult to maintain such a clear distinction between intelligence duties and other duties. The Committee would like to remark that although the heading of the draft new Section 65 a in the Police Databases Act only mentions ‘intelligence purpose’, it is apparent from the second paragraph that the information collected can also be used to open a prevention case or for investigation purposes. Such a general possibility to transfer information to other purposes would mean that the collection actually already serves (if the proposed amendment becomes law) all three purposes that PST is intended to serve. This would make the entire collection system a far more powerful tool for PST, and thus potentially also a far greater interference with protection of privacy, than the heading of Section 65 a would suggest.

In the Committee's opinion, such blurring of the distinction between PST's police and intelligence activities will have consequences for matters of principle, law and fact. From an oversight perspective, it would have been advantageous to look into this aspect in greater detail.

2.2 General discussion of bulk collection and automated data processing as interference with privacy

When information is processed for intelligence purposes, the Ministry proposes to stipulate in the Regulations that processing can be done using ‘automated analysis tools’, cf. the proposed new Section 21-8 second paragraph of the Police Databases Regulations. The use of automated analysis tools raises legal, technical and oversight-related issues.

As the Ministry writes,⁴⁹ collection and storage of publicly available information about individuals may constitute an interference with the right to respect for privacy (the Norwegian Constitution Article 102 and the European Convention on Human Rights (ECHR) Article 8), particularly if the collection is systematic and information is stored over time. In the consultation paper, the Ministry reviews case law from the European Court of Human Rights (ECtHR), including the judgments in the cases *Big Brother Watch v. the UK* and *Centrum för Rättvisa v. Sweden* from 2021. The Ministry states that these judgments have limited value because they concern covert surveillance as opposed to bulk collection from open sources. The Committee would nevertheless like to see a more detailed assessment of the judgments’ value in relation to the Ministry's proposal. In the above-mentioned judgments, the ECtHR has developed a set of assessment criteria that are better adapted to the collection of large quantities of data (bulk collection) than previous case law. The principle of end-to-end safeguards is particularly important.⁵⁰ Although the two cases in question concerned foreign intelligence (communication across national borders), many of the considerations are equally relevant to domestic intelligence, which is traditionally considered even more intrusive.

⁴⁸ Proposition No 80 to the Storting (Bill) (2019–2020) Lov om Etterretningstjenesten, section 9.3.3.

⁴⁹ Consultation paper sections 3.4.1 and 5.2.1.

⁵⁰ *Big Brother Watch* par. 350, *Centrum för Rättvisa* par. 264.

It is true that there is a material difference between the collection and storage of secret and openly available information. The Committee nevertheless considers the difference less significant than the consultation paper seems to suggest. Reference is made to Big Brother Watch par. 330,⁵¹ in which it is stated that 'the need for safeguards will be all the greater where the protection of personal data undergoing automatic processing is concerned'. It is also written in Big Brother Watch par. 342:⁵² 'Furthermore, any intrusion occasioned by the acquisition of related communications data will be magnified when they are obtained in bulk, since they are now capable of being analysed and interrogated so as to paint an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with (see paragraph 317 above).'

The use of automated analysis tools will generate new data about individuals that the person has not chosen to make openly available.

The Committee cannot see that the legal, technical and oversight-related issues relating to the use of automated analysis tools have been assessed.

2.3 On conditions for collection of openly available information

The intelligence mandate is accompanied by legal authority for PST to 'process openly available information', cf. the proposed new Section 65 of the Police Databases Act. The Ministry describes this as 'bulk collection and processing of openly available information'.⁵³ The Ministry assumes that PST will process large quantities of information 'much of which will not be of particular interest to PST'.⁵⁴

It is not clear from the consultation proposal whether introducing separate legal authority for the collection method has been considered, as is done in the Intelligence Service Act Section 6-2. The Committee would like an assessment of the need to enshrine the collection of openly available information in law as a method for PST.

The Committee understands the proposal to mean that the condition set for the collection and processing of large quantities of publicly available information is that it is 'necessary' for 'intelligence purposes' / 'intelligence activities', cf. the proposed new Section 65 a and new Section 64 third paragraph sub-section 6. It is proposed that this information be exempt from the provisions of the Police Databases Act Section 6 (Requirements regarding the quality of data) and Section 7 (Processing of special categories of personal data).

The Ministry sees that the proposal raises 'significant concerns relating to protection of privacy'⁵⁵ and that it will result in PST 'being able to process information about a large proportion of the population'.⁵⁶ The Committee questions whether further conditions should be stipulated for this interference in order to safeguard the privacy and due process protection of citizens - and, by extension, to ensure that real oversight by the Committee is possible.

2.4 On the use of information collected for intelligence purposes for other purposes

The proposed new provision in the Police Databases Act Section 65 a is headed processing of openly accessible information for 'intelligence purposes'. After the information has been collected, the Ministry proposes allowing the information to be 'used' for another two purposes:

⁵¹ Corresponds to *Centrum för Rättvisa* par. 244.

⁵² Corresponds to *Centrum för Rättvisa* par. 256.

⁵³ Consultation paper section 5.2.4.

⁵⁴ Consultation paper section 5.2.2

⁵⁵ Consultation paper section 5.2.1.

⁵⁶ Consultation paper section 5.2.6.

- To open or use in a preventive case
- For use by PST in the service's investigation duties

Such use of information from bulk collection in concrete cases will constitute a new and more serious interference with affected persons' right to protection of personal data and privacy. If the thinking behind the most recent judgments from the ECtHR is to be applied, further due process guarantees should be applied at this stage. Consideration for the Committee's oversight indicates that it should be defined what 'use' of information collected for intelligence purposes in preventive cases means and on what conditions personal data can flow between these tracks.

2.5 On deletion of information

The proposed new Section 65 a third paragraph of the Police Databases Act states that information collected from open sources is to be deleted after 15 years. The Committee would like grounds to be given to justify this deadline. In the assessment of how long information can be stored for, the Committee considers it relevant to emphasise that storage becomes more intrusive in relation to individual citizens the longer the information is stored.

The EOS Committee has discussed issues relating to the deletion of information stored by PST in its annual reports for 2001–2004, 2007–2012 and 2017. Some technical questions relating to deletion remain unclarified. The Committee would like to point out that when introducing a new method with a maximum deadline for deletion, it is important that a functioning deletion functionality is in place in PST's systems before the collection of information commences. It must also be possible for the EOS Committee to oversee the deletion functionality.

2.6 On restriction of access to information

The proposed new Section 65 a second paragraph of the Police Databases Act states that access to the information will be restricted. In principle, it is positive that information from bulk collection via open sources is kept separate from other information stored by PST and that clear restrictions on access apply. Although this does not constitute 'registration' in the sense of the Police Databases Act, such restricted processing nevertheless entails a form of information storage that should be governed by clear rules. The EOS Committee has discussed issues relating to the restriction of access to information stored by PST in its annual reports for 2012, 2014, 2015 and 2017. Some legal and technical issues relating to such restriction remain unclarified.

The Committee would also like to point out that, when introducing a new method where restriction of access to information constitutes a key part of the regulation regime, it is important that an adequate restriction functionality is in place in PST's systems before the collection of information commences. It must also be possible for the EOS Committee to oversee the restriction functionality.

2.7 On facilitation of the Committee's oversight

Section 6 of the consultation paper refers to the fact that PST will need ICT systems to store and analyse open information collected. PST must also facilitate oversight of its systems by incorporating possibilities for oversight into the systems. This should be done in consultation with the Committee to ensure that its oversight requirements are met. This also applies to any automated analysis tools. The Committee refers to the final paragraph of the Intelligence Service Act Section 7-11.

2.8 On budgetary consequences for the EOS Committee

The Ministry assumes that the proposal will not have budgetary consequences for the EOS Committee. However, if the proposed rules are adopted, the Committee's oversight of PST will

become considerably more demanding. It will also have a bearing on the Committee's resource requirements if further conditions for collection, storage, use and deletion of information are added, as called for here by the Committee.

The EOS Committee's oversight capacity can to a certain extent be increased by strengthening the Secretariat, as was done in connection with the Committee's new oversight responsibilities under the Intelligence Service Act. The Committee could also need technical equipment and software for training and data analysis for oversight purposes. If new and demanding tasks are assigned to the EOS Committee, however, that will also challenge the framework for the work of the Committee itself and its involvement in the different aspects of oversight.

Yours faithfully,

Astri Aas-Hansen
Chair of the EOS Committee

Appendix 4 – Consultation submission on the proposed amendments to the Police Databases Regulations

The Ministry of Justice and Public Security
 Attn. the Police Department
 P.O. Box 8005 Dep.
 NO-0030 OSLO

11 May 2021

Our ref.: 2021/276-2

Your ref.: 21/1564 - NNO

Consultation submission from the EOS Committee – Proposed amendments to the Police Databases Regulations

1. Introduction

Reference is made to the Ministry of Justice and Public Security's consultation letter of 19 March 2021 on proposed amendments to the Police Databases Regulations. The EOS Committee hereby submits its consultation submission.

The EOS Committee conducts subsequent oversight of PST. It is a prerequisite for genuine and effective oversight that the service has recorded its assessments and decisions in writing. Regarding the proposed amendment to Section 20-2, the Ministry writes that 'in any case, it must be documented that the service meets the statutory requirements that apply to processing of information'. The Committee shares this opinion. The Committee has also noted that the purpose of the proposed amendments is, among other things, to simplify the regulations 'without altering their material content'.

In light of the concrete amendments proposed to the provisions that regulate written documentation in the service, the Committee has nevertheless found reason to submit some comments.

2. Comments to individual amendments proposed

2.1. To the proposals for amendment to the Police Databases Regulations Sections 20-2 and 21-4

Regarding the proposal to remove the requirement for specification of purpose from Section 20-2 third paragraph, the Ministry writes that 'in any case, it must be documented that the service meets the statutory requirements that apply to processing of information'. Regarding the proposal to remove what is now Section 21-4 in its entirety, the Ministry writes that these factors must be considered in any case.

As regards intelligence registrations (processing of information outside the context of prevention cases), the EOS Committee agrees that the Police Databases Regulations Section 20-2 third paragraph is superfluous *in combination* with the Police Databases Regulations Section 21-4, which also requires specification of purpose. The requirement set out in Section 21-4 for what is referred to as a 'working hypothesis' also entails an assessment of necessity and relevance.

Oversight of intelligence registrations is one of the Committee's most important oversight responsibilities. Regarding the proposal to remove the requirement for specification of purpose from Section 20-2, the Ministry writes that the purpose '[will] as a rule in any case be apparent from the context of the processing'. From an oversight perspective, the EOS Committee does not share this view. It is particularly in the oversight of the *lower threshold* for intelligence registration, where precisely contextual information is sparse, that the specification of a working hypothesis (including specification of purpose) has an important function to fill.

The EOS Committee is of the opinion that the current requirements for a working hypothesis to be formulated, as set out in the Police Databases Regulations Section 21-4, should be upheld.

2.2. To the proposal for amendment to the Police Databases Regulations Section 22-3 third and fourth paragraphs

Subject to certain conditions, PST currently has a legal basis for continuing to process (i) intelligence registrations *to which no new information has been added in the past five years* and (ii) *concluded* prevention cases.

The Ministry proposes removing the requirement for decisions to continue to store information after the deadline set for deletion to be documented in writing. The Ministry refers to the fact that Section 47-14 stipulates no such requirement for written documentation and cannot see any reason for having different case processing rules for this type of case.

The Police Databases Regulations Section 47-14 regulates the deletion of information from the police's criminal intelligence register. Unlike the criminal intelligence register, individuals have no possibility to demand access to PST's registers and thus safeguard their own interests. In the Committee's opinion, this warrants different case processing rules.

The Committee is of the opinion that there is good reason to require grounds to be given for continuing to process *concluded* prevention cases and intelligence registrations *with no new information*. PST's decisions on continued storage of information that falls into these categories are routinely checked by the EOS Committee. That grounds are given and the decisions recorded in writing are an important prerequisite for the Committee being able to exercise effective and real oversight of the conditions for continued processing being met.

The EOS Committee considers that the current requirement for documentation should be upheld.

2.3. To the proposal for amendment to the Police Databases Regulations Section 21-5

The Ministry proposes simplifying this provision and expresses the opinion that much of it gives the impression of being a description of procedure. Among other things, it is proposed that the requirement for written documentation be removed.

The EOS Committee finds it difficult to see how the head of PST/chief of police would be able to approve a prevention case without a written record of the assessments that formed the basis for the case being opened. The Committee is nevertheless of the opinion that it has some value that a regulatory requirement is stipulated for decisions of such importance to be recorded in writing.

The EOS Committee considers that the requirement for written documentation should be upheld.

3. Concluding comments

The requirement for documentation in PST's activities constitutes such a fundamental guarantee of due process protection that it should warrant regulation in regulations, and not solely in the form of internal procedures. Overall, a weakening of the documentation requirements could impede the Committee's oversight and thus weaken individuals' due process protection.

The EOS Committee urges the Ministry to facilitate the Committee's oversight in its further regulatory work.

Yours faithfully,

Svein Grønnern
Chair of the EOS Committee

Appendix 5 – Input to the Storting's consideration of the Harberg Committee's report

The Standing Committee on Scrutiny and Constitutional Affairs
Stortinget
P.O. Box 1700 Sentrum
NO-0026 OSLO

Copy: The Presidium of the Storting

Our ref.: 2021/265

Your ref.:

24 March 2021

Input to the Storting's consideration of Document 21 (2020–2021)

1. Background

The Harberg Committee submitted its report to the Storting on the Storting's supervisory functions⁵⁷ on 1 February 2021. The EOS Committee wishes to submit some comments on parts of the report that directly impact the EOS Committee's activities.

2. The Committee's remarks

2.1 Proposed changes to the term of office for members of the EOS Committee

The Harberg Committee proposes changing the term for which committee members are appointed from five to four years, with the possibility of being re-appointed once. This would entail a reduction of the total length of service possible from ten to eight years.

The office of a member of the EOS Committee is complex and demanding. It takes time to familiarise oneself with and develop sufficient understanding and knowledge of the EOS field. The members have a limited amount of time at their disposal and, for security reasons, they do not have continuous access to the material subject to oversight. In the EOS Committee's opinion, this indicates a need for the greatest possible degree of continuity among the committee members.

More frequent replacement of committee members would also increase the number of people granted access to the EOS services' information. In our assessment, this is also an argument against reducing the members' term of office.

The EOS Committee is of the opinion that the Oversight Act Section 3 should not be amended as proposed by the Harberg Committee.

2.2 Proposal regarding fixed-term position for and appointment of the head of the secretariat

The Harberg Committee proposes that the head of the secretariat should be appointed by the EOS Committee itself, and not by the Presidium of the Storting on the basis of a recommendation from the Committee as stipulated by the present Section 4 of the Oversight Act. It is also proposed that the position of head of the secretariat become a fixed-term position for a term of six years with the possibility of being re-appointed once for another six-year term.

⁵⁷ Document 21 (2020–2021) *Rapport til Stortinget fra utvalget til å utrede Stortingets kontrollfunksjon* ('Report to the Storting from the committee appointed to assess the Storting's supervisory function' - in Norwegian only)

The EOS Committee emphasises that the head of secretariat's function is the cornerstone of the support the secretariat provides to the Committee. It is therefore vital for the EOS Committee to have a head of secretariat who possesses the knowledge, integrity and ballast required to perform this function in the best possible manner over time.

In the EOS Committee's letter of 20 November 2019 to the committee appointed to assess the Storting's supervisory functions, we wrote as follows:

'It is stated in the preparatory works to the Oversight Act that "[t]he office of the secretariat is so important that the choice should be made by the Storting, not by the Committee itself". The Standing Committee on Scrutiny and Constitutional Affairs considered the matter in 2009 in connection with amendments to the Directive relating to Oversight of the Intelligence, Surveillance and Security Services in force at the time. The Standing Committee's view was that the head of the secretariat "shall still be appointed and his/her remuneration stipulated by the Presidium of the Storting".

As the secretariat has grown in size and been delegated more duties by the Committee, the consideration on which the rule is based would seem to be even more relevant today. The Committee is of the opinion that the greater responsibilities and duties that the head of secretariat has taken on in relation to the EOS services indicate that the position should still have the legitimacy that the support of the Storting brings.

The Committee does not find it to encroach on our independence that the head of the secretariat is appointed by the Presidium. Based on the above, it is the Committee's wish that our head of secretariat should also in future be appointed by the Presidium of the Storting on the basis of a recommendation from the Committee.'

The EOS Committee considers it vital that the head of the secretariat, who deals with the EOS services on a daily basis, enjoys a high degree of confidence among the services. The Committee is of the clear opinion that the position should still have the legitimacy that the support of the Storting brings.

The EOS Committee is of the opinion that the Oversight Act Section 4 should not be amended as proposed by the Harberg Committee.

The EOS Committee will naturally be at the committee's disposal to answer any further questions you may have.

Yours faithfully,

Svein Grønnern
Chair of the EOS Committee

Appendix 6 – Act relating to oversight of intelligence, surveillance and security services⁵⁸

Section 1. The oversight area

The Storting shall elect a committee for the oversight of intelligence, surveillance and security services (the services) carried out by, under the control of or on the authority of the public administration (the EOS Committee). The oversight is carried out within the framework of Sections 5, 6 and 7.

Such oversight shall not apply to any superior prosecuting authority.

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

The Storting can issue instructions concerning the activities of the 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 this Act. The Storting in plenary session may, however, order the Committee to undertake specified investigations within the oversight mandate of the Committee, and observing the rules and framework which otherwise govern the Committee's activities.

Section 2. Purpose

The purpose of the Committee's oversight is:

1. to ascertain whether the rights of any person are violated and to prevent such violations, 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 unduly harm the interests of society.
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 oversight activities should be exercised so that they pose the least possible disadvantage for the ongoing activities of the services.

The purpose is purely to oversee. The Committee shall adhere to the principle of subsequent oversight. The Committee may not instruct the bodies it oversees or be used by

them for consultations. The Committee may, however, demand access to and make statements about ongoing cases.

Section 3. The composition of the Committee

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. A member may be re-appointed once and hold office for a maximum of ten years. Steps should be taken to avoid replacing more than four members at a time. Persons who have previously functioned in the services may not be elected as members of the Committee.

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

Section 4. The Committee's secretariat

The head of the Committee's secretariat shall be appointed by the Presidium of the Storting on the basis of a recommendation from the Committee. Appointment 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 approved by the Presidium of the Storting.

Section 5. The responsibilities of the Committee

The Committee shall oversee and conduct regular inspections of the practice of intelligence, surveillance and security services in public and military administration pursuant to Sections 6 and 7.

The Committee receives complaints from individuals and organisations. On receipt of a complaint, the Committee shall decide whether the complaint gives grounds for action and, if so, conduct such investigations as are appropriate in relation to the complaint.

The Committee shall on its own initiative deal with all matters and cases 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 5.

⁵⁸ The act was last changed in June 2020.

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 in the first sentence when special reasons so indicate.

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 6. The Committee's oversight

The Committee shall oversee the services in accordance with the purpose set out in Section 2 of this Act.

The oversight shall cover the services' technical activities, including surveillance and collection of information and processing of personal data.

The Committee shall ensure that the cooperation and exchange of information between the services and with domestic and foreign collaborative partners is kept within the framework of service needs and the applicable regulations.

The Committee shall:

1. for the Police Security Service: ensure that activities are carried out within the framework of the service's established responsibilities and oversee the service's handling of prevention cases and investigations, its use of covert coercive measures and other covert information collection methods.

2. for the Norwegian Intelligence Service: ensure that activities are carried out within the framework of the service's established responsibilities.

3. for the National Security Authority: ensure that activities are carried out within the framework of the service's established responsibilities, oversee clearance matters in relation to persons and enterprises for which clearance has been denied, revoked, reduced or suspended by the clearance authorities.

4. for the Norwegian Defence Security Department: oversee that the department's exercise of personnel security clearance activities and other security clearance activities are kept within the framework of laws and regulations and the department's established responsibilities, and also ensure that no one's rights are violated.

The oversight shall involve accounts of current activities and such inspection as is found necessary.

Section 7. Inspections

Inspection activities shall take place in accordance with the purpose set out in Section 2 of this Act.

Inspections shall be conducted as necessary and, as a minimum, involve:

1. several inspections per year of the Norwegian Intelligence Service's headquarters.
2. several inspections per year of the National Security Authority.
3. several inspections per year of the Central Unit of the Police Security Service.
4. several inspections per year of the Norwegian Defence Security Department.
5. one inspection per year of The Army intelligence battalion.
6. one inspection per year of the Norwegian Special Operation Forces.
7. one inspection per year of the PST entities in at least two police districts and of at least one Norwegian Intelligence Service unit or the intelligence/security services at a military staff/unit.
8. inspections on its own initiative of the remainder of the police force and other bodies or institutions that assist the Police Security Service.
9. other inspections as indicated by the purpose of the Act.

Section 8. Right of inspection, etc.

In pursuing its duties, the Committee may demand access to the administration's archives and registers, premises, installations and facilities 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.

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

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. The head of the respective service and the Chief of Defence may submit protests following such decisions. Protests as mentioned here shall be included in or enclosed with the Committee's annual report.

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 12. If in doubt, the provider of the information should be consulted.

Section 9. 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 being levied at 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 or her 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 11 and 16.

Section 10. Ministers and ministries

The provisions laid down in Sections 8 and 9 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.

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

Should the EOS 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. Duty of secrecy, etc.

With the exception of matters provided for in Sections 14 to 16, the Committee and its secretariat are bound to observe a duty of secrecy.

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 have the highest level of security clearance and authorisation, both nationally and according to treaties to which Norway is a signatory. The Storting's administration is the security clearance authority for the Committee's members and secretariat. The Presidium of the Storting is the appellate body for decisions made by the Storting's administration. The authorisation of the Committee's members and secretariat shall have the same scope as the Committee's right of inspection pursuant to Section 8.

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

Section 12. Procedures

Conversations with private individuals shall be in the form of an examination unless they are merely intended to 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 9. In connection with examinations in cases that may result in criticism being levied at 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 the evidence and claims are unclassified, or the person has authorised access.

Section 13. Quorum and working procedures

The Committee has a quorum when five members are present.

The Committee shall form a quorum during inspections of the services' headquarters as mentioned in Section 7, but may be represented by a smaller number of members in connection with other inspections or inspections of local units. At least two committee members must be present at all inspections.

In connection with particularly extensive investigations, the procurement of statements, inspections of premises, etc. may be carried out by the secretariat 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 examinations as mentioned in this Section, the Committee may engage assistance.

Section 14. On the oversight and statements in general

The EOS Committee is entitled to express its opinion on matters within the oversight area.

The Committee may call attention to errors that have been committed or negligence that has been shown in the public administration. If the Committee concludes that a decision must be considered invalid or clearly unreasonable or that it clearly conflicts with good administrative practice, it may express this opinion. If the Committee believes that there is reasonable doubt relating to factors of importance in the case, it may make the service concerned aware of this.

If the Committee becomes aware of shortcomings in acts, regulations or administrative practice, it may notify the ministry concerned to this effect. The Committee may also propose improvements in administrative and organisational arrangements and procedures

where these can make oversight easier or safeguard against violation of someone's rights.

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 15. Statements to complainants and the public administration

Statements to complainants should be as complete as possible without disclosing classified information. Information concerning whether or not a person has been subjected to surveillance activities shall be regarded as classified unless otherwise decided. Statements in response to complaints against the services concerning surveillance activities shall 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 service or 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. Otherwise, statements concerning complaints shall always be sent to the head of the service against which the complaint is made.

Statements to the administration shall be classified according to their contents.

Section 16. Information to the public

The Committee shall decide the extent to which its unclassified statements or unclassified parts of statements shall be made public.

If it must be assumed that making a statement public will result in the identity of the complainant becoming known, the consent of this person shall first be obtained. When mentioning specific persons, consideration shall be given to protection of privacy, including that of persons not issuing complaints. Civil servants shall not be named or in any other way identified except by approval 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.

Public access to case documents that are prepared by or for the EOS Committee in cases that the Committee is considering submitting to the Storting as part of the constitutional oversight shall not be granted until the case has been received by the Storting. The EOS Committee will notify the relevant administrative body that the case is of such a nature. If such a case is closed without it being submitted to the Storting, it will be subject to public disclosure when the Committee has notified the relevant administrative body that the case has been closed.

Section 17. Relationship to the Storting

The provision in Section 16, first and second subsections, correspondingly applies to the Committee's notifications and annual reports to the Storting.

Should the Committee find that 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.

The Committee submits annual reports to the Storting about its activities. Reports may also be submitted if matters are uncovered that should be made known to the Storting immediately. Such reports and their annexes shall be unclassified. The annual report shall be submitted by 1 April every year.

The annual report should include:

1. an overview of the composition of the Committee, its meeting activities and expenses.
2. a statement concerning inspections conducted and their results.
3. an overview of complaints by type and service branch, indicating what the complaints resulted in.
4. a statement concerning cases and matters raised on the Committee's own initiative.
5. a statement concerning any measures the Committee has requested be implemented and what these measures led to, cf. Section 14, sixth subsection.
6. a statement concerning any protests pursuant to Section 8 fourth subsection.
7. a statement concerning any cases or matters which should be put before the Storting.

8. the Committee's general experience from the oversight activities and the regulations and any need for changes.

Section 18. 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 to have been submitted by the Committee unless communicated in writing.

Section 18 a. Relationship to the Security Act

The Security Act applies to the EOS Committee with the exemptions and specifications that follow from the present Act, cf. the Security Act Section 1-4 first paragraph.

The following provisions of the Security Act do not apply to the EOS Committee: Sections 1-3, 2-1, 2-2 and 2-5, Chapter 3, Section 5-5, Section 7-1 second to sixth paragraphs, Section 8-3 first paragraph second sentence, Section 9-4 second to fifth paragraphs, Chapter 10 and Sections 11-1, 11-2 and 11-3. Within its area of responsibility, the EOS Committee shall designate, classify and maintain an overview of critical national objects and infrastructure and report it to the National Security Authority, together with a specification of the classification category, cf. the Security Act Section 7-1 second paragraph.

Within its area of responsibility, the EOS Committee may decide that access clearance is required for access to all or parts of critical national objects or infrastructure and decide that persons holding a particular level of security clearance shall also be cleared for access to a specified critical national object or specified critical national infrastructure, cf. the Security Act Section 8-3.

The Storting may decide to what extent regulations adopted pursuant to the Security Act shall apply to the EOS Committee.

Section 19. 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.

Persons who are employed by the services may not be engaged to provide assistance.

Section 20. Financial management, expense reimbursement for persons summoned before the Committee and experts

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.

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 Act No 2 of 21 July 1916 on the Remuneration of Witnesses and Experts.

Experts receive remuneration in accordance with the fee regulations. Other rates can be agreed.

Section 21. Penalties

Wilful or grossly negligent infringements of the first and second subsections of Section 8, first and third subsections of Section 9, first and second subsections of Section 11 and the second subsection of Section 19 of this Act shall render a person liable to fines or imprisonment for a term not exceeding one year, unless stricter penal provisions apply.