COMMISSIE VAN TOEZICHT
BETREFFENDE
DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

REVIEW REPORT

on

THE OFFICIAL MESSAGES
ISSUED BY GISS IN THE PERIOD
OCTOBER 2005 UP TO AND INCLUDING MAY 2010

CTIVD NO. 29

28 September 2011

REVIEW COMMITTEE
FOR THE
INTELLIGENCE AND SECURITY SERVICES

CTIVD no. 29

REVIEW REPORT

On the official messages issued by GISS
in the period October 2005 up to and including May 2010

Table of contents

REVIEW COMMITTEE
FOR THE
INTELLIGENCE AND SECURITY SERVICES

CTIVD no. 29

SUMMARY

of the review report on the official messages issued by GISS in the period October 2005-May 2010

The Committee's investigation was directed at the official messages which GISS issued in the period from October 2005-May 2010. Based on the explanatory memorandum to the ISS Act 2002 the Committee has used the following definition of 'official message': the provision of information to a recipient who is authorized to take measures as a result of this information against the person or organisation mentioned in the message. In its investigation the Committee assessed, as it did in its first investigation of the official messages of GISS, whether the official messages issued by GISS satisfy the statutory requirements regarding the processing and external provision of (personal) data. In addition, the present investigation paid attention to the use made of the official messages in the follow-up procedures.

In view of the large number of official messages assessed by the Committee and the long period covered by the investigation, the Committee has only a limited number of critical remarks.

The official messages issued to the Public Prosecution Service, the Immigration and Naturalization Service (INS) and the category of 'other recipients' such as mayors and chiefs of police, generally satisfy the statutory requirements. The remarks of the Committee regarding these categories of official messages concern isolated defects, not structural ones. With respect to one official message issued to the INS the Committee holds the opinion that the indicated reliability regarding part of the information provided is not supported by the underlying file. In this respect, the official message is unlawful. In a number of cases, moreover, the Committee holds the opinion that GISS should have exercised greater care in formulating the text of the official message. Furthermore, the Committee has commented with respect to official messages issued to the Public Prosecution Service and the INS that the GISS should as far as possible seek to provide concrete, factual information, bearing in mind, of course, the need to keep secret its sources, its current level of knowledge and/or the operational methods of the service.

The official messages issued by GISS to the ministry of Economic Affairs, Agriculture and Innovation (EAA&I) in the context of applications for export permits are of a different nature than the aforementioned categories. These official messages are classified state secret, and they are to a certain extent standardized in nature. During the first part of the review period GISS did not consider this type of information provision to constitute official messages. Partly for this reason GISS initially did not observe the statutory requirements very strictly. The Committee has established, however, that GISS has improved its procedure in recent

years, with the result that they are now acting in compliance with the statutory requirements.

The fact that the official messages issued to the ministry of EAA&I are classified is not consistent with the basic principle of the ISS Act 2002 that an official message may be inspected without any objections by the person or organisation to which it relates. The Committee holds the opinion, however, that the classification of this category of official messages is justified, because the information provided will by definition reveal the knowledge level of GISS regarding companies in so-called countries of concern. It is important, though, that GISS is aware of the drawbacks associated with the classification of official messages, both for the ministry of EAA&I, which bases its decision wholly or partly on secret information, and for the exporter concerned who is not in a position to question the statements of GISS. In consultation with the ministry of EAA&I GISS must therefore try and find ways to promote that the ministry can take its decisions on the basis of an adequate information position. One possibility is to grant the ministry inspection of the documents underlying the official messages where necessary.

The Committee has included two categories of information provision in its investigation which previously were not classed as official messages. These are the category of provision of information to political party chairpersons concerning holders of or candidates for political office and the category of provision of information to the person charged with forming a new government or the prime minister on candidates for government posts. GISS may provide information on holders of or candidates for political office in response to a request for information from the party chairperson. GISS then provides the party chairperson with information obtained by an administrative check concerning the person in question in the databases of GISS. Prior to providing information on candidates for government posts GISS always does an administrative check at the request of the person charged with forming a new government or the prime minister. The Committee holds the opinion that these forms of information provision fall under the term 'official message' as defined by the Committee.

The messages concerning holders of or candidates for political office issued to political party chairpersons and the official messages concerning candidates for government posts issued to the person charged with forming a new government or the prime minister have certain structural shortcomings as regards both policy and implementation.

A particular shortcoming in official messages issued to party chairpersons is the absence of an indication of reliability or source reference, while in some cases personal data were provided orally instead of in writing. In addition, GISS wrongly considers doing an administrative check in its own databases in response to a request for information from a party chairperson to be a form of data provision. The Committee points out to GISS that the legal basis for such administrative checks is not the article of law pertaining to the provision of data, but the article of law pertaining to data processing in general. This means that doing an administrative check in response to a request from a party chairperson must be necessary for the performance by GISS of its tasks, in the interest of national security. The Committee has found that there were three cases in which there was insufficient legal basis for the administrative checks done by GISS.

As regards the official messages to the person charged with forming a new government or the prime minister the Committee has found that GISS, contrary to the statutory provisions on the external provision of personal data, has opted for a policy of providing the

information orally. As a result, and because of the absence of a report on the oral provision of information in 2007, it was impossible for the Committee to find out on which candidate for a government post information was provided in this period.

The Committee points out that it is precisely the political sensitivity of the provision of information concerning holders of or candidates for political office and candidates for government posts that is an urgent reason for thoroughly laying down all steps in writing.

REVIEW COMMITTEE
FOR THE
INTELLIGENCE AND SECURITY SERVICES

CTIVD no. 29

LIST OF ABBREVIATIONS

belonging to the review report on the official messages issued by GISS in the period October 2005 up to and including May 2010

CT Infobox	Counterterrorism Infobox
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EAA&I	(ministry of) Economic Affairs, Agriculture and Innovation
GALA	General Administrative Law Act
GISS	General Intelligence and Security Service
INS	Immigration and Naturalisation Service
ISS Act 1987	Intelligence and Security Services Act 1987 (old)
ISS Act 2002	Intelligence and Security Services Act 2002
Sv	Code of Criminal Procedure
WMD	weapons of mass destruction

REVIEW COMMITTEE
FOR THE
INTELLIGENCE AND SECURITY SERVICES

CTIVD no. 29

REVIEW REPORT

on the official messages issued by GISS in the period October 2005 up to and including May 2010

1 Introduction

Every year the General Intelligence and Security Service (GISS) issues a great number of official messages to bodies which are authorised to act on the information contained in the official message by taking measures. Essentially, therefore, the investigations carried out by GISS serve the purpose of giving the responsible bodies early warning against possible threats to the interests mentioned in the mandate of GISS.[1]

The Intelligence and Security Services Act 2002 (ISS Act 2002) does not contain a definition of the term 'official message'. The explanatory memorandum to the bill introducing the ISS Act 2002 contains a discussion of the term:

> "If it is to be expected on the basis of the information to be provided that the competent authority will take measures against the person concerned which will prejudice his legitimate interests, the information must be provided in a written (unclassified) official message. […] The basic principle is, that in the case of providing information to parties outside the circle of intelligence and security service, the information must be provided to the authority which is authorised to take measures for the preventive protection of the interests concerned or to take repressive action against impairment of the interests."[2]

Based on these passages the Review Committee for the Intelligence and Security Services (further referred to as: the Committee) arrives at the following definition of the term 'official message': the provision of information to a recipient who is authorised to act on the information by taking measures against the person or organisation mentioned in the message.

In 2006 the Committee issued a report on the official messages issued by GISS in the period from January 2004 - October 2005. The results of the Committee's investigation were mainly positive. The Committee's final conclusion was in fact that the official messages issued by GISS in that review period were in accordance with the law and had been prepared in an appropriate manner and with proper and due care.[3]

---

[1] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 55.
[2] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 55.
[3] Review report of the Committee no. 9a on the official messages issued by the AIVD in the period from January 2004 – October 2005. *Parliamentary Papers II* 2005/2006, 29 924, no. 9 (annex), final observation. Also available at www.ctivd.nl.

Because of the increased use and importance of official messages in judicial proceedings, the Committee announced in the report that it would monitor the official messages of GISS on a regular basis. Such monitoring means that the Committee regularly examines the official messages that have been issued together with the corresponding files in the light of a number of statutory requirements (see section 3). As a result of the first findings of this monitoring the Committee decided to do a new in-depth investigation, so that it could conduct a more thorough investigation of the issues that had arisen upon a first reading of the official messages and underlying files. The present review report is the result of this investigation. The investigation paid particular attention to the use made of the official messages in the follow-up procedure.

By letter of 5 April 2007 this follow-up investigation of official messages was announced to the minister of the Interior and Kingdom Relations and the presidents of the two Chambers of the Dutch parliament. Initially, the investigation was aimed at the official messages issued in the period from October 2005 up to and including January 2007. After the investigation had been at a standstill for some time, mainly due to several time-consuming investigations instituted at the request of the minister of the Interior and Kingdom Relations[4] and the minister of Defence[5] and partly because the Committee's secretariat was short of staff, the Committee decided to extend the investigation to include the period from February 2007 up to and including May 2010. Consequently, this review report covers the official messages issued by GISS in the period from October 2005 up to and including May 2010.

The Committee drafted the review report on 10 August 2011 and sent it to the minister of the Interior and Kingdom Relations, requesting a reaction before 15 September 2011. On 27 September 2011 the Committee received a letter containing the minister's reaction to the draft report. The Committee adopted the review report on 28 September 2011.

2 Organisation of the investigation

The Committee included all provisions of information falling under the above definition of the term official message in its investigation. Two categories of information provision which were previously were not classed as official messages, were now included in the present investigation. These are the category of provision of information to political party chairpersons on holders of or candidates for political office and the category of provision of information to the person charged with forming a new government or the prime minister on candidates for government posts.

In the course of its investigation the Committee examined the files of 566 official messages, checking whether they complied with the statutory requirements pertaining to data processing, and more specifically the requirements pertaining to the external provision of (personal) data. Three requirements played a key role in the investigation:

[4] Review Report of the Committee no. 17 on the assessment processes at GISS with respect to Mohammed B., *Parliamentary Papers II* 2007/08, 29 854, no. 22 (annex). Also available at www.ctivd.nl.
[5] Review report of the Committee no. 25 on the conduct of DISS with respect to two suspended employees, *Parliamentary Papers II* 2010/11, 29 924, no. 59 (annex). Also available at www.ctivd.nl.

1. the official message must have its basis in Article 36, 38 or 39 of the ISS Act 2002;
2. the official message must be substantiated by the underlying information;
3. the official message must contain an indication of the reliability of the information or a reference to its source.

Insofar as there was reason for doing so, the Committee also investigated the lawfulness of how the data incorporated in the messages had been processed. Such processing may take the form, for example, of an administrative check by GISS in its own databases or the use of special powers.[6]

Another point for attention in the process of examining the files was the transparency of the files, since that is important element of internal accountability for the information provision and its external monitoring. A transparent and complete file is moreover an important basis enabling GISS to prepare an official message with due care.

In addition to examining the files, the Committee conducted interviews with lawyers employed at GISS. Some official messages were also discussed with employees and heads of the teams that drafted the official messages. The Committee spoke with an employee of the ministry of Economic Affairs, Agriculture and Innovation (EA&I) about the official messages issued to this ministry. The Committee also talked with two national public prosecutors for counterterrorism (further referred to as 'national public prosecutors') about the official messages issued to the Public Prosecution Service and with the head of a Regional Intelligence Service. Furthermore, the Committee also interviewed an employee of the Immigration and Naturalisation Service (INS), who works at GISS as the Service's liaison officer (further referred to as: the INS liaison).

When the first review report on the official messages of GISS was presented to the States General, the minister promised that GISS would adopt the Committee's recommendations in full. In the review report on the follow-up by GISS to the recommendations, the Committee established that GISS had taken action on all recommendations regarding the official messages, in particular those concerning the adjustment of internal rules.[7] In the present review report these recommendations will only be discussed insofar as the internal rules or their implementation give the Committee cause for further comments.

The review report has the following structure. Section 3 sets out the legal framework for issuing official messages. Sections 4 through 9 then discuss the different categories of recipients of official messages and the findings of the Committee. The relevant case law is reviewed in the process. Section 10 contains the conclusions and recommendations of the Committee.

This review report has no secret annex.

---

[6] During the review period the Committee also regularly (and separately) monitored the lawfulness of the use of the special powers under Articles 25 and 27 ISS Act 2002. See for an explanation of the structural monitoring activities of the Committee the Committee's annual report 2010-2011, available at www.ctivd.nl.

[7] Review report of the Committee no. 18a on the fulfilment by GISS of the commitments made by the minister of the Interior and Kingdom Relations in response to the recommendations of the Committee. *Parliamentary Papers II* 2007/08, 29 924, no. 25 (annex). Also available at www.ctivd.nl.

3 Legal framework for issuing official messages

3.1 Data processing generally

The law sets three requirements for data processing generally – the external provision of data is one of the types falling in this category – which are laid down in Article 12 ISS Act 2002 (paragraphs 2, 3 and 4). In the first place data may only be processed for a specific purpose and only insofar as necessary for the proper implementation of the ISS Act 2002 or the Security Screening Act. Secondly, data processing must take place in accordance with the law and with proper and due care. The last general requirement is that the data must be provided together with an indication of the degree of reliability or a reference to the document or source from which the information is derived.

These three general requirements will be further elaborated below and discussed specifically with regard to official messages.

3.1.1 For a specific purpose and insofar as necessary

The origin of the requirement that data may only be processed for a specific purpose and only insofar as necessary for the proper implementation of the ISS Act 2002 or the Security Screening Act lies partly in a comparable provision in the ISS Act 1987,[8] the legislation that was the basis for the activities of the predecessor of GISS, the National Security Service.[9] In the ISS Act 2002 the requirement that data may only processed for a specific purpose was added to the requirement of necessity under the influence of the bill containing the Personal Data Protection Act, which included a provision that personal data may only be collected for specific, expressly defined and legitimate purposes.[10] [11]

Partly in reaction to two judgments of the Administrative Jurisdiction Division of the Council of State in which it was ruled among other things that the existing rules for inspection of personal data recorded by the National Security Service did not satisfy the requirements of the European Convention on Human Rights (ECHR),[12] rules were inserted into the ISS Act 2002 about the inspection of data processed by or for the use of the services (Articles 45-57 ISS Act 2002).[13] Furthermore, it was decided in response to a recommendation in the final report of the Parliamentary Committee of Inquiry into Investigation Methods (Van Traa Committee)[14] to create an explicit legal basis in the ISS Act 2002 for the provision of data to the Public Prosecution Service for the purposes of the investigation and prosecution of offences (Article 38 ISS Act 2002).[15] At the same time a legal basis was included for the provision of data, for urgent and serious reasons, to persons or bodies designated by or pursuant to a general administrative measure and charged with a public

---

[8] Article 16(1) ISS Act 1987.
[9] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 19.
[10] *Parliamentary Papers II* 1997/98, 25 892, no. 1, p. 3 (Article 7).
[11] *Parliamentary Papers II* 1997/98, 25 877, no. 8, p. 41.
[12] Administrative Jurisdiction Division of the Council of State 9 June 1994, *AB* 1995/238 (Van Baggum).
[13] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 3.
[14] *Parliamentary Papers II* 1995/96, 24 072, no. 11, p. 441.
[15] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 58.

task (Article 39 ISS Act 2002). These statutory provisions pertain to activities of GISS which do not serve the interest of national security, though they do serve a public interest. Consequently, these activities fall outside the statutory description of tasks of GISS under to Article 6(2) ISS Act 2002.

In the light of this extension of the statutory activities of GISS compared to those of the National Security Service, the scope of the necessity requirement was also adjusted so that it does not only apply to data processing for the purpose of performing the statutory tasks – in the interest of national security – but also to the other forms of data processing provided for by or pursuant to the ISS Act 2002 or the Security Screening Act.[16] The wording chosen for Article 12(2): "necessary for the proper implementation of this Act or the Security Screening Act" comprises all statutory activities of GISS. However, the necessity requirement operates differently in the case of data processing for the purpose of the own task of GISS than in the case of data processing for the purpose of activities outside the own task of GISS.

When GISS issues an official message for the purpose of performing its tasks (Article 36 ISS Act 2002), providing the data to the body authorised to take measures against a person or organisation must be necessary in the interest of national security. In addition, providing the data must also serve a specific purpose. It emerges from the legislative history that this requirement relates to how the service actually performs its tasks.[17] Providing data pursuant to Article 36 ISS Act 2002 must therefore fit in with the way in which GISS actually performs its tasks.

Providing the Public Prosecution Service with data that may be important for the investigation or prosecution of offences (Article 38 ISS Act 2002) and providing persons and bodies charged with a public task with data for an urgent and serious reason (Article 39 ISS Act 2002) are activities that fall outside the statutory tasks of GISS. In such cases data is provided for the purpose of the recipient's task. For those forms of data provision, the combination with the requirement of necessity leads to the requirement that providing the data must be necessary for the purpose of the task of the recipient body, with a view to the measures to be taken by that body. GISS obviously has only limited insight into the information position of the recipient body, so that the service cannot be expected to assess to what extent the data to be provided is essential for the recipient for it to be able to take measures. To the extent that the service does have an insight into the importance of the information, it must include this aspect in its assessment. In this context the liaisons of the recipient bodies play a role. Both the Public Prosecution Service and the Immigration and Naturalisation Service (INS) employ persons whose tasks include the task of monitoring cooperation with GISS. Two national public prosecutors and two INS officers act as liaisons.

The legislative history of the ISS Act 2002 shows that when GISS assesses whether it is necessary to issue an official message, it must include the nature and seriousness of the facts in its assessment and also the weighty interests involved and the possible consequences for the person concerned, in particular if fundamental rights may be at issue.[18] This means that whenever it is assessed whether it is necessary to issue an official message, an element of

[16] The Explanatory Memorandum to the bill containing the ISS Act 2002 shows that the general provisions on data processing by the services pertain to data processing for the purpose of the performance by the service of its tasks and to other forms of processing provided for by or pursuant to the ISS Act 2002 or the Security Screening Act (*Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 18).
[17] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 19.
[18] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 55.

proportionality enters the picture as well, since the seriousness of the facts and the weighty interests to be served by the information provision must be balanced against the possible consequences for the person concerned.

3.1.2 In accordance with the law and with proper and due care.

With regard to official messages, the requirement that data processing must take place in accordance with the law and with proper and due care means in the first place that the official messages must satisfy the requirements set for such messages pursuant to section 3.3 of the ISS Act 2002.

In the context of official messages, the requirement of proper and due care concerns the procedure followed to make the message. Making an official message with proper and due care requires first of all that the text of the message is based on information in the possession of GISS. An official message is only lawful when its text is substantiated by the underlying information. The thorough preparation of a file containing all the documents on which the text of the message is based is one of the safeguards on this point. As the Committee observed in its first review report on the official messages of GISS, the transparency of data processing will benefit by the addition of a supplementary memorandum to each file, which contains references to the documents on which the official message is based.[19]

In addition to the substantiation of the information provided, the accuracy of the text of an official message is also important:

> "It is self-evident that it is a compelling duty of the services to guarantee the exactness and accuracy of the information provided."[20]

The fact that GISS must carefully choose the wording of an official message follows from the requirement that data processing must take place with proper and due care. An official message must contain an accurate, factual presentation of the underlying information and must, moreover, be as clear as possible, so that it is not capable of different interpretations. At the same time it must be borne in mind that GISS must also take account of its statutory duty to ensure that sources qualifying for secrecy are in fact kept secret and its duty to ensure the safety of the persons cooperating in the collection of information (Article 15 ISS Act 2002). In some cases it may be necessary for the service to make the text of the message slightly less specific so that it cannot be deduced from the text that the information derives from a specific technical or human source.

One aspect which, in the opinion of the Committee, is related to the provision of information with proper and due care is, that the internal procedure for making official messages should provide for the necessary control mechanisms to ensure the accuracy and exactness of the information. For this purpose the law imposes a specific statutory duty on the head of the service to ensure that the necessary arrangements are in place to promote the accuracy and completeness of the data that is processed (Article 16(a) ISS Act 2002).

---

[19] Review report of the Committee no. 9a on the official messages issued by GISS in the period from January 2004 – October 2005. *Parliamentary Papers II* 2005/06, 29 924, no. 9 (annex), section 3.3. Also available at www.ctivd.nl.

[20] *Parliamentary Papers II* 1997/98, 25877, no. 3, p. 55.

Article 38(3) ISS Act 2002 provides with regard to official messages to the Public Prosecution Service that the appropriate officer of this Service is authorized to inspect all information underlying the official message which he needs to be able to assess the accuracy of the message. This provision is another safeguard that data processing takes place with proper and due care.

3.1.3 Indication of reliability or source reference

For the recipient of an official message, who may possibly proceed to take measures against the party concerned, it is relevant to know what is the quality of the data provided by GISS. Article 12(4) ISS Act 2002 therefore provides that the data processed by the service in the context of the performance of its task must be accompanied by an indication of reliability or a reference to its source. The simplest way of satisfying this requirement is to include a source reference in the official message. It will be clear, however, that where secret methods have been used to collect the data, it is impossible to refer to the source without disclosing information on the operational methods of the service or without acting in violation of the obligation of secrecy and the obligation to ensure the safety of the persons who cooperated in collecting the data (Article 15 ISS Act 2002). In such cases the service must choose the option of indicating the reliability of the data in the text of the official message. This indication of reliability may take different forms. Two of the indications used by GISS are: "GISS has reliable information" and "GISS has information […]. The reliability of this information could not be established." For the recipient body this indication of reliability is essential to being able to assess on the merits whether or not to take measures.

The statutory obligation to indicate the reliability of information means that GISS, before issuing an official message, must assess the reliability of the information in its possession. This assessment should be made using procedures which, in conformity with Article 16(a) ISS Act 2002, promote the accuracy and the completeness of the data that have been processed. An example of such a procedure is the use of data from different sources if it possible to do so. Often, moreover, GISS will already have acquired the necessary knowledge in this area in the course of the investigation from which the information originates, thus making it possible for the employees concerned to form a sound opinion of the reliability of the information. When the information originates from a human source, it is important for GISS to critically evaluate its cooperation with the source on a periodic basis. Pursuant to Article 21 ISS Act 2002, agents are subjected to periodic evaluation anyway in connection with the three-monthly renewal of the agent's deployment. In addition, the internal rules require that a brief memorandum on the source is drawn up to be included in the file underlying the official message, which states what is the basis of the reliability assessment (further referred to as: reliability memorandum). In point of fact the reliability memorandum forms (part of) the substantiation of the indication of reliability.

3.2 Processing of personal data

Article 13(1) of the ISS Act 2002 contains an exhaustive list of the categories of persons whose personal data GISS may process. In addition to data relating to persons who are investigation targets in the context of the tasks of GISS, GISS may also process personal data of persons about whom data has been collected by other intelligence or security services, or whose data

is necessary to support the proper performance by the service of its tasks, or who are or have been employed by the service.

Data relating to a person's religion or belief, race, health or sexuality may only be processed supplementary to the processing of other data and exclusively if this is required for the purpose of processing such other data (article 13(3) and (4), ISS Act 2002).

3.3 External provision of data

For the purposes of GISS' tasks, in the interests of national security, various powers have been conferred on GISS that it can use to collect (personal) data in secret and privacy-infringing ways. It follows that the data collected by GISS may only be disclosed externally in the interests of national security or because of another weighty interest such as the investigation and prosecution of offences. For this reason the ISS Act 2002 has a closed system of data provision, which means that data may only be disclosed externally if a specific statutory basis exists for doing so. Consequently, GISS may only issue an official message pursuant to Article 36, 38 or 39 of the ISS Act 2002 and in accordance with the requirements set for issuing official messages in the ISS Act 2002.

As was already briefly discussed in section 3.1.1, the law provides that information may be provided for two reasons. In the first place, an official message may be issued in the context of proper task performance, that is to say for the purpose of the tasks of GISS, in the interests of national security. The basis for the provision of information in the context of the performance by GISS of its task is Article 36 ISS Act 2002. These are cases in which the responsible body must be informed well in time so that it can take measures against a person or organisation who or which is the subject of the official message. Such a measure can e.g. be the refusal of an export permit application for exports that would contribute to the proliferation of weapons of mass destruction (WMD) or an order declaring a person forming a threat to national security to be an undesirable alien. Other examples of such measures are the sanction of freezing financial assets or refusing permission to hold a demonstration.

Secondly, GISS may provide information in the context of the task of the recipient. There is a specific legal basis (Article 38 ISS Act 2002) for the provision of data that is important for the investigation and prosecution of offences. Such data is provided to the member of the Public Prosecution Service designated for this purpose, namely the National Public Prosecutor. Although this Article and the Explanatory Memorandum to the Bill containing the ISS Act 2002 show that the provision relates to a discretionary power of the minister of the Interior and Kingdom Relations to provide data to the Public Prosecution Service, it will be clear that the discretionary margin decreases as the gravity of the offence increases.[21] The Committee further points out that one must not lose sight of the reason for allowing the service this discretionary margin in assessing whether or not to provide data to the Public Prosecution Service; one of the factors to be taken into account is the extent to which providing data could adversely affect an investigation of GISS or the performance by GISS of its tasks, generally.

Finally, Article 39 ISS Act 2002 constitutes a legal basis for the provision of data that is relevant to other public tasks than investigating or prosecuting offences. Since the principle of the closed system of information provision calls for restraint in providing data for the

[21] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 58.

purposes of interests other than those of national security, Article 39 ISS Act 2002 sets two conditions for such data provision: (1) data may be provided only to persons or bodies designated by general administrative measure and involved in performing a public task and (2) there must be an urgent and serious reason for providing the data.

Pursuant to Article 39 ISS Act 2002, the following persons and bodies have been designated by general administrative measure: the ministers, the Dutch Central Bank (De Nederlandsche Bank N.V.), the Dutch Authority for the Financial Markets (Stichting Autoriteit Financiële Markten) and the mayors insofar as the data to be provided relates to their responsibility for public order and insofar it relates to their advisory task regarding nominations for a royal honour (Designation Order pursuant to Article 39 ISS Act 2002).[22] It rarely happens that official messages are issued pursuant to Article 39 ISS Act 2002. This is in keeping with the expectation, expressed when the bill containing the ISS Act 2002 was discussed in parliament, that the services would in practice make sparing use of the power laid down in Article 39.[23]

3.4 External provision of personal data

Articles 40, 41 and 42, ISS Act 2002, set a number of additional requirements for the provision of personal data. The reason for additional requirements is that it is appropriate to exercise special due care because the provision of personal data very emphatically affects the privacy of the person concerned.[24]

The main rule is that personal data is provided in writing where the recipient is competent to act on the data by taking measures against the person concerned (Article 40(1) ISS Act 2002). Personal data may only be provided orally in case of urgency. Written confirmation should follow as soon as possible in such cases (Article 40(2) ISS Act 2002).

By way of additional safeguard for the accuracy and reliability of the personal data to be provided Article 41(1) ISS Act 2002 provides that the service may not provide personal data whose accuracy cannot reasonably be established or which was processed more than ten years ago, while no new data has been processed regarding the person in question since that time. Derogation of this provision is possible in the case of the provision of personal data to the Public Prosecution Service, to counterpart services of GISS and in other special cases to be determined by the minister of the Interior and Kingdom Relations (Article 41(2) ISS Act 2002). When data is provided in derogation of the provision of Article 41(1), the degree of reliability and the age of the data must be stated (Article 41(3) ISS Act 2002).

Article 42 ISS Act 2002, finally, provides that records must be kept of the provision of personal data. In its previous review report on official messages issued by GISS the Committee already came to the conclusion that this obligation to keep records is complied

---

[22] Order of 22 September 2004 designating persons and bodies pursuant to Article 39(1) of the Intelligence and Security Services Act 2002 (Designation Order pursuant to Article 39 ISS Act 2002), *Stb.* 2004, 506, amended by order of 21 November 2006 amending general administrative measures in connection with the introduction of the Financial Supervision Act, *Stb.* 2006, 663.
[23] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, p. 35.
[24] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 59.

with through the retrievable storage of the official messages at GISS.[25] This makes it possible for both the service and the Committee to retrieve what personal data was provided to which recipient.

4 Official messages to the Public Prosecution Service

4.1 Use of official messages to the Public Prosecution Service

The role that information from the intelligence and security services can play in criminal process was discussed as early as in February 1992 in connection with the former National Security Service in a letter sent by the minister of Justice to the Second Chamber of Parliament.[26] This letter first deals with the difference between collecting intelligence and investigating crimes. It is explained that intelligence is collected in the interest of national security regardless of the existence of an offence or suspected offence.

The ISS Act 2002 emphasizes the distinction by providing that officers of the services do not have powers to investigate offences (Article 9(1) ISS Act 2002). The distinction between intelligence collection and crime investigation does not imply, however, that information in the possession of National Security Service should not be useful for criminal law enforcement. The distinction can, however, give rise to a different assessment of the information for evidential purposes. Ultimately, this assessment is made by the criminal court.[27]

In conclusion, the aforementioned letter to the Second Chamber mentions the following uses of information from the National Security Service:

a) the information can constitute reason to start a criminal investigation;
b) the communicated facts and circumstances can result in a legitimate suspicion within the meaning of Article 27 of the Dutch Code of Criminal Procedure;
c) the information can constitute legal proof within the meaning of the Code of Criminal Procedure.[28]

Decisions have been given on this issue in Case Eik, first by the Court of Appeal of The Hague and subsequently by the Supreme Court. On 21 June 2004 the Court of Appeal of The Hague ruled that the Public Prosecution Service and the criminal court may in principle assume that GISS performed its task lawfully and duly placed its official messages at the disposal of judicial authorities. Not only can information from GISS form the basis for starting a criminal investigation, it can also be the basis for arresting the suspect.[29] The

[25] Review report of the Committee no. 9a on the official messages issued by GISS in the period from January 2004 - October 2005, *Parliamentary Papers II* 2005/06, 29 924, no. 13 (annex), section 4.8. Also available at: www.ctivd.nl.
[26] When the ISS Act 2002 was discussed in parliament, the minister stated that broadly considered this letter was still an accurate and useful presentation of how data from the intelligence and security service can be used in criminal investigations. *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 12.
[27] *Parliamentary Papers II* 1991/92, 22 463, no. 4, p. 2.
[28] *Parliamentary Papers II* 1991/92, 22 463, no. 4.
[29] Court of Appeal The Hague 21 June 2004, *NJ* 2004, 432 / *LJN*: AP3601 and AP2058 (case Eik), para. 4.3.10.

Supreme Court confirmed this trend in its judgment of 5 September 2006, adding that in principle there are no objections to using material gathered by intelligence and security services in criminal proceedings. The criminal courts, so the Supreme Court states, are deemed to assess carefully on a case-by-case basis whether the material can form part of the evidentiary material, having regard to the sometimes limited review possibilities.[30] The Committee notes that the new rules on hearing identity-protected witnesses are intended to enhance the evidential value of official messages (see section 4.2).

The Supreme Court mentions a number of situations in which information from GISS may in any case not be taken into account in weighing the evidence.[31] For example: it is not permitted to deliberately not use investigative powers with a view to bringing about that criminal-law safeguards will not apply so that information from GISS can be used or continued to be used. Furthermore, the acts of GISS may not restrict the fundamental rights of the suspect to such extent that there is no longer question of a fair trial as referred to in Article 6 of the ECHR. Finally, the court must examine whether the limited possibilities of reviewing the information from GISS do not restrict the rights of the defence to such extent that using the information in evidence results in violation of the fair trial requirement of Article 6 ECHR.

The use of information from GISS in the criminal process was once again the subject of extensive discussions in the Second Chamber in the context of the bill containing the Witness Identity Protection Act.[32] It was emphasized that the extent to which the reliability of the information stated in an official message can be verified will affect the use of information from GISS as evidence.[33] The Second Chamber also discussed the issue of GISS' continuing to provide information after a criminal investigation has been started. In this situation a distinction must be made between the provision, at the request of the Public Prosecution Service, of intelligence already collected by GISS, and the collection of intelligence at the request of the Public Prosecution Service followed by the provision of this intelligence.[34] The former information provision is permitted, the latter conflicts with Article 9(1) ISS Act 2002. The Supreme Court quoted this explanation in a case involving the continued exchange of information between GISS and the Public Prosecution Service after a criminal investigation had been started. The defence complained that the investigations had become intermingled. The Supreme Court ruled that there is no rule of law precluding parallel investigations with GISS continuing to provide information, so long as there is cause to continue the intelligence investigation for the purposes of the performance by GISS of its task. In the case in question the Supreme Court held that it was not an incomprehensible decision of the Court of Appeal that evidently the available information was cause for GISS to continue its intelligence investigation.[35]

[30] Supreme Court 5 September 2006, *LJN*: AV4144 (case Eik), para. 4.6.
[31] Supreme Court 5 September 2006, *LJN*: AV4144 (case Eik), paras. 4.7.2 and 4.8.
[32] *Parliamentary Papers II* 2003/04, 29 743, no. 3.
[33] *Parliamentary Papers II* 2003/04, 29 743, no. 3, p. 5.
[34] *Parliamentary Papers II* 2004/05, 29 743, no. 7, p. 23.
[35] Supreme Court 13 November 2007, *LJN*: BA2553 (animal rights activist), paras. 3.4.1-3.5.3, also: Court of Appeal The Hague 2October 2008, *LJN*: BF3987 (case Piranha).

4.2 The Witness Identity Protection Act

In 2002 the District Court of Rotterdam, in a judgment that was subsequently set aside by the Court of Appeal of The Hague[36], held that information from GISS may serve as initial information at the start of criminal proceedings, but that a person may not be considered a suspect within the meaning of Article 27 of the Dutch Code of Criminal Procedure (also referred to as "Sv") exclusively on the basis of an official message from GISS.[37] Shortly after this judgment it was decided to prepare for an amendment to the Code of Criminal Procedure. The proposal formed part of a package of changes in the law to combat terrorism.

On 1 November 2006 the Act amending the Code of Criminal Procedure (witness identity protection) (further referred to as the Witness Identity Protection Act) entered into force.[38] The purpose of this change in the law is to increase the usefulness of official messages of GISS in the criminal process. Where formerly an official message could only be used in evidence in combination with other evidence, it now constitutes full documentary evidence (Article 344 Sv). It is subsequently for the court to further examine its reliability so that it can establish its evidential value. For this purpose the court may e.g. hold that it needs to hear an employee of GISS. At a public hearing, however, this employee will usually have to invoke his obligation of secrecy (Article 85 ISS Act 2002). The examining magistrate of the District Court of Rotterdam has exclusive jurisdiction to hear identity-protected witnesses under the witness identity protection regime (Article 178a(3) in conjunction with Articles 226m-226s Sv), in which case the minister of the Interior and Kingdom Relations can release the GISS employee concerned from his obligation of secrecy (Article 86(2) ISS Act 2002). In principle, the defence and the public prosecutor handling the case do not have the right to be present at the hearing, but they may submit questions (Article 226p, paragraphs (1) and (4) Sv). The identity-protected witness himself assesses whether the interest of national security precludes furnishing the report of the witness hearing to the parties in the proceedings and including it in the documents of the case (Articles 226p(3) and 226s(1) Sv). If the witness does not assent to the report being furnished, it is destroyed and the examining magistrate makes a note of the fact in a new report. It is the responsibility of the examining magistrate to include an opinion on the reliability of the statement made by the identity-protected witness in the report (Article 226q Sv). Since the amendment of Article 187d Sv, the examining magistrate himself can now also prevent, when he prepares the report, that answers to questions concerning specific data come to the notice of the public prosecutor, the suspects and his counsel if there are good reasons to believe that this would harm the interest of national security (Article 187d(1)(c) Sv). Based on the report of the witness hearing and the examining magistrate's opinion on the reliability of the witness' statement, the trial judge then establishes the persuasive power of the official message.

Since the entry into force in 2006 of the Witness Identity Protection Act no use has been made yet of the opportunity to hear GISS employees as identity-protected witnesses.[39] In the criminal cases in which the evidential value of official messages came up for examination, the means provided by the Witness Identity Protection Act for further examining the

---

[36] Court of Appeal The Hague 21 June 2004, *NJ* 2004, 432 / *LJN*: AP3601 and AP2058 (case Eik).
[37] District Court of Rotterdam 18 December 2002, *LJN*: AF2141 (case Eik).
[38] Act amending the Code of Criminal Procedure (witness identity protection), 28 September 2006, *Stb.* 2006, 460. Entry into force: 1 November 2006 (*Stb.* 2006, 461).
[39] See in this connection also the cabinet report on counterterrorism measures in the Netherlands in the first decade of the 21st century (*Antiterrorismemaatregelen in Nederland in het eerste decennium van de 21ste eeuw*), published in January 2011, annex H, p. 88.

evidential value of official messages were not applied.[40] So far, the rules on hearing witnesses under the partial anonymity regime (Article 190(2) SV) have been used when GISS employees were heard. Partial anonymity means that the examining magistrate can direct that questions about particular facts shall not be asked, if there are good reasons to believe that the witness will suffer nuisance in connection with his having given evidence or will be impeded thereby in the performance of his duties. In the fairly recent case concerning the leaking of information to daily newspaper De Telegraaf, the examining magistrate inspected the documents underlying the official message in question pursuant to the authority of Article 187d Sv.[41]

The minister of Justice has undertaken to report to the States-General on the effectiveness and the effects of the Act in actual practice. The Research and Documentation Centre is currently carrying out an assessment. The assessment is expected to be completed in the third quarter of 2011.[42]

4.3 Procedure for making official messages to the Public Prosecution Service

The National Public Prosecutor has been designated as the recipient of official messages issued to the Public Prosecution Service. This officer passes on the official messages to the appropriate public prosecutor's office. This can be a district public prosecutor's office, the National Public Prosecutors' Office or the National Public Prosecutor's Office for Financial, Economic and Environmental Offences. In 2006 a second National Public Prosecutor was appointed.

When information has emerged from an investigation by GISS which qualifies for being provided to the Public Prosecution Service, the team concerned usually consults with the National Public Prosecutor. This officer then informs GISS whether in his opinion the information is useful for the Public Prosecution Service. If it is, the team prepares a draft text and collects the underlying documents. Subsequently, the text of the official message together with the underlying documents is discussed and agreed with the legal department of GISS. In situations where GISS has identified an acute threat, it may happen that no prior coordination with the National Public Prosecutor takes place.

The legal department is responsible for ensuring agreement on the text of the official message between the National Public Prosecutor and the team. The National Public Prosecutor examines among other things whether the wordings used in the official message are sufficiently factual and unambiguous. It is not the intention that the text already contains criminal characterizations of facts, since it is the task of the court to assess whether criminal characterizations apply on the basis of the available factual information. If necessary, the parties concerned can consult about making changes in the text of the official message. As soon as agreement has been reached on the text of the official message, the team will complete and put the file in order. The internal rules at GISS prescribe that the author of the official message must prepare an overview to accompany the file.

---

[40] For example District Court Rotterdam 1 December 2006, *LJN*: AZ3589 (Samir A. a.o.), Court of Appeal The Hague Den Haag 2 October 2008, *LJN*: BF3987 (case Piranha, Samir A. a.o.).
[41] District Court Haarlem 14 July 2010, *LJN*: BN1191 and *LJN*: BN1195 (Telegraaf leak)
[42] *Parliamentary Papers I* 2010/11, 32 500 VI, no. L, p. 4.

After the team head and the legal department have approved the official message and the accompanying file, the message is presented to the National Public Prosecutor together with the file. The check done by the National Public Prosecutor at this stage concerns the accuracy of the official message (Article 38(3) ISS Act 2002). Accuracy means that the text is substantiated by the underlying documents. In addition, the National Public Prosecutor pays attention to the accuracy of the indication of reliability. It is emphatically not for the National Public Prosecutor to assess the truth of the information; that task is reserved for the criminal court. Neither does the National Public Prosecutor review whether the underlying information has been gathered lawfully. The judgments of the District Court of Haarlem in the case concerning the leaking of state-secret information to daily newspaper De Telegraaf show that the National Public Prosecutor must check whether the message is correct by reference to the underlying documents before the official message is issued, unless it is demonstrated that there was no time to do so on account of the circumstances.[43]

After the National Public Prosecutor has checked whether the official message is correct, it is presented together with the file to the head of the unit to which the team in question belongs. The National Public Prosecutor is notified of any adjustments in the text of the official message. Finally, the official message is signed and adopted by the head or deputy head of GISS.

4.4 Findings of the Committee

4.4.1 The number of official messages in the review period

The Committee has established that GISS issued 132 official messages to the Public Prosecution Service in the review period. These official messages thus account for 23% of the total number of official messages issued in this period. The annual number of official messages issued to the Public Prosecution Service varies, but averages approximately 30 official message per year.

4.4.2 Legal basis

The legal basis for issuing official messages relating to offences to the Public Prosecution Service is Article 38 ISS Act 2002. In the opinion of the Committee, all but one of the official messages issued by GISS to the Public Prosecution Service are rightly founded on this basis.

In 2006 GISS issued an official message which in the Committee's opinion should not have been issued to the Public Prosecution Service on the basis of Article 38. The official message was issued in connection with the results of a security screening by GISS of a civil servant who had applied for a position of confidentiality. In the course of the security screening, facts became known about the civil servant which were not fitting for a person holding a position of confidentiality, but which were also not fitting for the position the civil servant already held at the time. The civil servant was confronted with the facts and decided to withdraw his application for the position of confidentiality, as a result of which GISS did not complete the security screening. Because GISS believed that the activities of the civil servant were

[43] District Court Haarlem 14 July 2010, *LJN*: BN1191 and *LJN*: BN1195 (Telegraaf leak). At the time of adopting the present review report the case was still pending before the appeal court.

incompatible with the position the civil servant was holding at the time, and that those activities might impair the integrity of the organisation in which the civil servant was employed, GISS decided to issue an official message. The official message was issued to the National Public Prosecutor, stating that the reason was that it could not be excluded that the civil servant had not declared the possible secondary income from the activities to the Tax Authorities, which in the opinion of GISS had given rise to a suspicion of tax evasion.

The Committee holds the opinion that GISS wrongly issued this official message to the Public Prosecution Service. The fact is that GISS did not know whether the activities had actually generated income, nor was there evidence of any other offences. Moreover, the National Public Prosecutor had already notified GISS that it would not prosecute the person concerned. The Committee endorses the opinion of GISS that the activities of the civil servant were incompatible with his position. Since impairment of the integrity of public administration may in some cases also constitute a danger to the continued existence of the democratic legal order, or to national security or other serious state interests, GISS could have sent the official message to the employer pursuant to Article 36 ISS Act 2002.[44] In the opinion of the Committee, however, GISS should not have issued the official message to the Public Prosecution Service.

4.4.3 Necessity

As was already explained in section 3.1.1, providing information to the Public Prosecution Service with a view to measures to be taken must be necessary for the purposes of the task of the Public Prosecution Service: the investigation and prosecution of offences. In the course of its investigation the Committee came across two cases in which GISS provided data to the Public Prosecution Service which the Service already possessed. GISS was in fact aware of this. It concerns official messages issued in 2007 and 2010. In both cases the Committee found that by issuing the messages GISS sought to influence the follow-up steps to be taken by the Public Prosecution Service.

The first case concerned information from the police which had been reported to GISS via the Regional Intelligence Service. Because GISS considered the threat to be serious, it subsequently provided the information to the National Public Prosecutor to induce the Public Prosecution Service to take action. GISS thus acted contrary to its own internal rules which direct that regular police information is not included in official messages except in exceptional cases. GISS must then state expressly in the official message that the information had been provided to GISS pursuant to Article 62 ISS Act 2002, which in this case it did not do.

In the other case GISS intended to exert influence on the choice of the service that was to carry out the investigation. GISS considered it important for the investigation in question to be conducted by the National Police Internal Investigations Department, while at that moment it was also possible that the Public Prosecution Service would choose to keep the investigation within its own organisation and have it carried out by a unit of the National Public Prosecutor's Office for Financial, Economic and Environmental Offences. By issuing the official message GISS wished to stress the seriousness of the case and thus influence the choice of the service that was to carry out the investigation. The Committee observes on this point that it finds it understandable that GISS, which at the time of issuing an official

[44] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, p. 33 and *Parliamentary Papers II* 2005/06 VII, no. 47.

message has often already invested many months – if not years – in the case, wishes to ensure that the body to which it provides the information handles the case in a certain way. However, issuing an official message containing information that is already known to the recipient is not the appropriate procedure for achieving this. When GISS has specific wishes or advice concerning the steps which the Public Prosecution Service should undertake in a certain investigation, it can consult with the Service – through the National Public Prosecutor. The Committee holds the opinion that in such cases providing information is not necessary for the purpose of the investigation and prosecution of offences since the Public Prosecution Service already has the information.

The Committee has established that situations may exist in which GISS chooses to provide information to the Public Prosecution Service while it has already been made clear to GISS through the National Public Prosecutor that the Service does not consider it expedient or sees no possibility to act on the information. Taking into consideration its above observations, the Committee advocates that in such a situation GISS first tries to reach agreement through the existing hierarchical channels.

4.4.4 Content

The Committee has found that the content of the official messages issued by GISS to the Public Prosecution Service in the review period is substantiated by the underlying files. In a number of cases, however, GISS did not draft the text of the message with sufficient care.

In 2008 GISS issued an official message which in the opinion of the Committee contains a confusing passage. In this official message GISS stated among other things that there was concrete evidence that the person concerned was involved with certain activities. This was based amongst other things on the suspected presence of the person concerned at certain meetings. The Committee holds the opinion that qualifying as concrete evidence the information in question, which related to events which were suspected to have taken place, creates confusion. This wording does not make clear to the recipient how strong the evidence is.

In a comparable case, in an official message issued in 2005, GISS informed the Public Prosecution Service that the person concerned belonged to a certain group. Investigation by the Committee showed that this assertion could not be fully substantiated by the available information. In view of the scanty information on the contacts between the person concerned and members of the relevant group, it is the opinion of the Committee that GISS should have chosen a wording that was more in keeping with the actual findings.

An official message issued by GISS in 2008 reported that the person concerned, who was being associated with terrorist activities, seemed to be in contact with another person *in this context.* After studying the file, the Committee found that GISS only had information that the two persons were registered at the same address. Upon enquiry at GISS it turned out that the service wished to indicate that the person concerned was in contact with the other person and that in this context the other person also required (or might require) the attention of the Public Prosecution Service. It is the opinion of the Committee that in this case, too, GISS should have formulated the text of the message with greater care.

In some other official messages the structure of the text leads to a lack of clarity. One official message issued in 2006 states that the information in the message was obtained from more

than one source. A list of information follows. It is not clear to the reader whether each item of the information originates from one or from several sources. Another example is an official message issued in 2009, which states in the first sentence that the information is reliable. Further on in the official message only the word information is used, so that it is not clear whether this is information that is justly qualified as "reliable information".

Of the two other cases in which the Committee hold the opinion that GISS did not exercise sufficient care, one message stated an incorrect house number and the other message an incorrect address. In both cases GISS had the correct information. The Committee points out that including incorrect address details may have serious consequences, for example if the Public Prosecution Services decides to carry out a police raid at the (incorrect) address stated by GISS.

4.4.5 Deciding to provide information to the Public Prosecution Service

As a result of two detailed official messages which GISS issued to the Public Prosecution Service in 2009, the legal experts of GISS discussed the fact that the Public Prosecution Service is increasingly asking GISS for detailed official messages. Subsequently, the policy line in this field was laid down in an internal memorandum. Pursuant to this memorandum GISS may only comply with a request for a detailed official message if there are urgent reasons in the context of the tasks of GISS to bring about that the criminal investigation gets a speedy start. GISS will not be allowed to comply with such a request from the Public Prosecution Service if this would harm the interests of GISS, such as protecting its operational methods.

The Committee holds the opinion that this reasoning is at odds with the intention of the legislature. In the Explanatory Memorandum to the bill containing the ISS Act 2002 it is explained that the underlying reason for the margin of appreciation allowed GISS in deciding whether or not to provide information to the Public Prosecution Service is, that the proper performance by the service of its task would be impeded if they would have to notify the Public Prosecution Service each time it identified an offence. It follows that GISS, in deciding whether or not to provide information to the Public Prosecution Service, must assess to what extent this will harm the performance of its own task, taking account of the possibility that the Public Prosecution Service will decide to investigate and prosecute. If GISS only provides detailed information when national security urgently calls for a matter to be investigated and prosecuted, then GISS exercises greater restraint than was envisaged by the legislature. The Committee points out that the interests of investigation and prosecution must carry great weight. Whenever it is possible for GISS to reveal (detailed) information, it should only decide not to do so if providing the information would harm the interests of the service.

4.4.6 Indication of reliability or source reference

In its investigation the Committee established that as a rule GISS consistently includes an indication of reliability in the official messages to the Public Prosecution Service.

Two related official messages issued in 2006 are an exception to this rule. These messages merely mention information without characterising its reliability. The Committee has found that GISS wished to leave it to the Public Prosecution Service to characterise the information,

in order not to interfere with the investigation that had already been started. The Committee points out that characterising the reliability of information must be distinguished from characterising the information itself. The former is a statutory duty for GISS, while it may refrain from the latter if it is appropriate to do so in view of the obligation of secrecy or the demarcation of the tasks of the service.

Another case in which GISS did not include an indication of reliability is an official message issued in 2008. This proved to be a deliberate choice of GISS. The information that was the reason for issuing the message, which was considered reliable, originated from a foreign counterpart service and GISS was not permitted to distribute the information on account of international agreements on further distribution. There were, however, also reports in the media that supported the information. In addition, GISS possessed certain information which it had obtained from its own investigations. By leaving out the indication of reliability, GISS in fact left it undecided on which information it had ultimately based the official message. The Committee finds that if GISS adhered to the agreement with the counterpart service, it did not provide the information originating from that service. This has the result that part of the official message is based on a media report only. This should have been clear from the text of the official message. With respect to information from publicly accessible sources the best choice is generally to mention the source, since this improves the transparency of the message.

In its first review report on the official messages of GISS the Committee explained that it is not necessary that information is confirmed by material from other sources for GISS to establish that information is reliable. This means that GISS can assess information from one single human source as reliable. In its investigation the Committee came across some examples of official messages to the Public Prosecution Service in which information from one single human source formed the basis of part of the message. The files of these official messages include memorandums on the reliability of the sources in question. The Committee holds the opinion that in these cases GISS exercised due care in establishing the reliability of the information.

4.4.7 Exculpatory information

Information qualified as reliable by GISS which contradicts the conclusion drawn in the official message, is called exculpatory information. GISS includes this information either in the official message or in the underlying file. If, however, GISS has information which it does not qualify as reliable but which contradicts the conclusion drawn in the official message, then GISS does not consider this to be exculpatory information. In such cases GISS will not mention the information in the official message nor include it in the underlying file.

In 2006 the Public Prosecution Service enquired at GISS, through the National Public Prosecutor, whether the service had exculpatory information concerning a person with respect to whom GISS had previously issued an official message. In reply to this request GISS issued an official message in which it explained how the accuracy and completeness of official messages are safeguarded by internal procedures. The Committee has established that this explanation leaves room for misunderstandings as far as the subject of exculpatory information is concerned. GISS stated in the official message that:

> "[…] in the case that we have contradictory information, the service will decide either to give expression to this in the wording of the official message or not to issue an official message

because the information is insufficiently reliable and consequently unsuitable for being mentioned in an official message."

This explanation creates the impression that information which GISS does not consider reliable but which contradicts the conclusion drawn in the official message, will nevertheless be included in the official message or may even have the result that no official message is issued. As was described above, this is not the procedure followed at GISS. The fact is that GISS, when drafting the official message, finds that such information must not be considered as exculpatory information. This assessment and the subsequent decision not to include the information in the official message fall within the statutory task of GISS.

The Committee wishes to point out, though, that because this information is not included in the underlying file, it will not be found by the National Public Prosecutor who checks the content of the official messages issued to the Public Prosecution Service. It will also not be possible for the Committee to review the assessment in retrospect. As a result, the assessments made by GISS regarding the reliability of this information are unverifiable. In the opinion of the Committee it is advisable to arrange the files underlying official messages in such a way that they show whether exculpatory information is available and how GISS assessed its reliability.

4.4.8 Lawfulness of the underlying data processing

In 2009 GISS issued two official messages to the Public Prosecution Service relating to the export practices of a specific company. A CD-ROM containing tapped telephone conversations was enclosed as an annex with each of the two messages. As a result of the official messages of GISS a criminal investigation was started in the course of which the criminal investigation team used telephone taps. The intelligence investigation of GISS, which also included the use of special powers, was continued as well. The latter investigation resulted among other things in a third official message to the Public Prosecution Service, in 2010. As a general observation it can be said that special powers may be used while a criminal investigation is going on at the same time as long as there is a lawful basis for such use (see section 4.1). In this situation, however, GISS must make sure that the needs of the Public Prosecution Service do not become the guiding factor in its intelligence investigation. On the other hand it is important that both GISS and the Public Prosecution Service obtain as complete a picture of the subject matter as possible. This requires coordination, with each party keeping its own task in mind while gaining an understanding of the other party's needs, so that the appropriate information can be provided. The Committee studied the reasons stated for the continued use of special powers in the investigation in question. It holds the opinion that this continued use was lawful from the intelligence perspective. It emerged from interviews held with employees of the service and with the National Public Prosecutor that regular consultations took place between the relevant GISS team and the criminal investigation team, under the leadership of the National Public Prosecutor. The Committee has found that due care was exercised in keeping the two parallel procedures strictly separate.

In addition, the Committee has seen cause to put further questions to GISS about the use of special powers in an investigation of GISS aimed at characterising a potential imminent threat to the democratic legal order. GISS had provided information to the National Public Prosecutor to be used by the criminal intelligence unit of the National Investigation Service, which was conducting an investigation of the group in question at the same time. The

Committee examined whether the use of the special powers satisfied the statutory requirements of necessity, proportionality and subsidiarity. The Committee holds the opinion that in view of the relevant facts and circumstances the powers were used lawfully, although the reasons stated in writing for the use of the special powers showed some defects.

4.4.9 Documentation

One of the safeguards for the careful making of an official message is the existence of a complete underlying file. The Committee has established that generally the official messages that have been issued to the Public Prosecution Service are supported by thorough documentation.

In one case GISS added an earlier official message on the relevant persons to the file of a subsequent official message to substantiate certain information. The Committee points out that the use of official messages in substantiation of other official messages entails the risk of losing sight of the age of the information that actually underlies the subsequent official message. It is the opinion of the Committee that in such cases GISS should add (copies of) the relevant documents from the file of the earlier official message to the new message file.

5 Official messages to the Immigration and Naturalisation Service (INS)

5.1 The use of official messages issued to the Immigration and Naturalisation Service

Pursuant to its statutory mandate, GISS has power to investigate whether threats exist to national security, including threats coming from aliens staying in the Netherlands. A decision of the INS to cancel or refuse a residence permit and/or an order declaring a person an undesirable alien, one of the criteria for which is whether the alien constitutes a threat to national security,[45] may therefore be based on an official message from GISS.

The European Court for Human Rights (ECtHR) has accepted in its case law that the states that are signatories to the ECHR do not further define the term 'national security' in their national legislations. The states are left a margin of appreciation when interpreting the term. This margin of appreciation is delimited by what can still be deemed to fall under the natural meaning of the term. The ECtHR has ruled, for example, that considering a person a threat to national security on the grounds of his involvement with drugs trafficking went beyond the natural meaning of the term 'national security'.[46]

If an official message from GISS shows objectively, impartially and clearly which facts and circumstances underlie the conclusion of the message and if this conclusion is not incomprehensible without further explanation, there is no reason for INS to inspect the documents underlying the official message.[47] So an official message can be considered an

[45] Cancellation of fixed-term residence permit: Article 32(1)(b) of the Aliens Act 2000; cancellation of permanent residence permit: Article 35(1)(d) of the Aliens Act 2000; order declaring a person an undesirable alien: Article 67(1)(c) of the Aliens Act 2000.
[46] ECtHR 24 April 2008 (*C.G. e.a./Bulgaria*), A 1365/07, para. 43.
[47] Administrative Jurisdiction Division of the Council of State 4 July 2006, *LJN*: AY3839, para. 2.1.4.

expert opinion, which means that INS may in principle assume that the information is accurate, unless there are concrete indications that there is reason to doubt the accuracy or completeness of the information.[48] It is the responsibility of the alien to allege any such indications.[49]

It is logical that the more concrete and detailed the facts and circumstances are described in the official message, the more readily INS will be able to conclude that the official message is clear and transparent and decide not to further investigate its content.[50] For the sake of clarity it must be noted in the context of the foregoing that INS remains responsible for stating the reasons for its decisions under aliens law.

For some years now GISS has also been issuing official messages to INS which do not include the conclusion "threat to national security". It follows from case law that these official messages must also be considered expert opinions.[51] By means of an official message INS can be informed, for example, of an alien's anti-integrative behaviour, where this falls within the scope of the mandate of GISS. Examples are persons who make statements directed against the democratic legal order or who incite to actions that are contrary to statutory and other rules.[52] This information from GISS can be used to constitute (part of) the basis for a decision refusing an application for being granted Dutch nationality or for withdrawing Dutch nationality.[53] It also happens that GISS provides information of a factual nature to INS, when there are reasons to suspect that a person has furnished incorrect data or has withheld information in the context of the grant or renewal of a residence permit. This type of data provision may only take place to the extent that providing the data is in the interest of national security. Derogation from this rule is only permitted if there is another urgent and serious reason to provide the data. In the latter case the data is provided to the minister for Immigration and Asylum pursuant to Article 39 ISS Act 2002.

In administrative procedures the court has the possibility of ascertaining that the conclusions in the official message are supported by the underlying file.[54] If the file underlying the official message includes documents that are classified state-secret, the minister of the Interior and Kingdom Relation will inform the court that only the court is authorised to inspect the underlying file.[55] This means that neither the alien concerned nor the government member concerned is granted inspection of the underlying documents at that stage. To satisfy the requirements of fair trial, Article 87(1) ISS Act 2002 provides that the court may only (partially) base its judgment on those documents with the consent of the parties. The possibility for the court to inspect the underlying file is important with a view to the case law

---

[48] Administrative Jurisdiction Division of the Council of State 12 October 2001, *LJN*: AD5964, para. 2.3.4 and District Court The Hague 12 June 2006, *LJN*: AY4303, para. 5.2.
[49] Administrative Jurisdiction Division of the Council of State 4 July 2006, *LJN*: AY3839, para. 2.1.4.
[50] District Court The Hague 28 May 2010, *LJN*: BM7552, para.7.
[51] Administrative Jurisdiction Division of the Council of State 29 September 2010, 201000881/1/V6, paras. 2.6.1 and 2.6.2 (Taraghini).
[52] Guide to the Netherlands Nationality Act, explanatory note to Article 8(1)(d) of this Act, section 3.3.
[53] This is effected pursuant to Article 8(1)(d) of the Netherlands Nationality Act (civil integration counter-indication) and/or Article 9(1)( )a of the same Act (serious suspicion of threat to public order, public morality or the security of the Kingdom).
[54] If the minister of the Interior and Kingdom Relations refuses to allow the court inspection of the underlying documents of the official message, the court may draw such conclusions as it deems fit from this fact (Article 8:31 of the Dutch General Administrative Law Act).
[55] Article 8:45 in conjunction with Article 8:29 of the General Administrative Law act read with Article 87(1) ISS Act 2002.

of the ECtHR, from which it ensues that a party whose treaty rights are infringed by a measure taken for the purposes of national security, must have the possibility of having the measure reviewed by an independent and impartial body that is authorised to examine all the relevant facts and issues of law.[56]

The fact that the alien himself will generally not be allowed to inspect the documents underlying the official message on account of their state-secret nature, may restrict his right to a defended action. This restriction does not by definition mean, however, that there can be no fair trial.[57] In order to stand the test of the ECtHR, however, the official message itself, which the alien may inspect, must contain sufficient concrete and specific information and thus give the alien sufficient reference points to be able to contest the information. In *A. e.a./United Kingdom* the ECtHR mentions as an example of a concrete reference point the allegation that the person concerned had attended a terrorist training camp at a stated location between stated dates.[58]

5.2 Procedure for making official messages to the Immigration and Naturalisation Service

In its first review report on the official messages issued by GISS the Committee considered it advisable, in view of the increased number of official messages to INS, that GISS would make sound arrangements with INS about a procedure for communicating with INS about official messages. It suggested that INS adopt a procedure providing for the designation of an officer who would act as permanent liaison with regard to official messages. This recommendation has had the result that since 2007 the INS liaison, who had previously been appointed as contact for operational matters, has been assigned a structural role in the procedure for making the official messages issued by GISS to INS. Recently, a second INS liaison was appointed.

The exchange of information between GISS and INS is regulated in greater detail in a covenant between the two services. The covenant provides – briefly stated – that the services may provide each other with data that can be relevant to the performance of their tasks. The covenant, which dates from 2003, adds little to the statutory provisions. Newer forms of cooperation, such as the provision of information in the context of the decision-making process under the Netherlands Nationality Act and the requests for information from INS to GISS, have not been incorporated in the covenant. At the time of drafting the covenant, moreover, the position of INS liaison at GISS did not yet exist. As early as in 2007, in its review report on the exchange of information between GISS and INS, the Committee already pointed out that the covenant needed to be revised. The reason why the revision has been postponed so far is that the services were awaiting an amendment of the ISS Act 2002 (the so-called post-Madrid measures), because this amendment was expected to result in a fundamental change in the basis for the cooperation between GISS and INS. Recently, however, the bill amending the ISS Act 2002 was withdrawn. The Committee therefore recommends that GISS, in consultation with INS, formalises the current practice of exchanging information between GISS and INS in a written procedure as soon as possible.

---

[56] ECtHR 20 June 2002 (*Al Nashif/Bulgaria*), A 50963/99, para. 123.
[57] ECtHR 20 July 2010 (*A./Netherlands*), A 4900/06, para. 160; ABRvS 7 October 2008, *LJN*: BG1209, para. 2.4.
[58] ECtHR 19 February 2009 (*A. a.o./United Kingdom*), A 3455/05, para. 220.

From the perspective of internal procedure the official messages which GISS issues to INS must be distinguished into two categories. The first category comprises official messages issued in reaction to an advice from the Counter-Terrorism (CT) Infobox, a cooperative group in the field of counter-terrorism and radicalism comprising *inter alia* GISS, DISS, INS, the Public Prosecution Service and the National Police Services Agency.[59] These are official messages concerning persons who are associated with terrorism and/or radicalism and who are for this reason included in the CT Infobox list. The employees of INS seconded to the CT Infobox have access to the information in the possession of GISS about persons on the list and can examine which information may be relevant for INS. This makes it possible to make an analysis based on the combined information of the two services and the information provision can be tailored to either the aliens law procedure or the naturalisation procedure.

The second category comprises the official messages not issued on the basis of an advice from the CT Infobox. These are official messages issued on the initiative of GISS or official messages issued in response to a request for information from INS. Apart from the INS employees seconded to the CT Infobox, INS has no insight into the information available at GISS. In the case of official messages not issued on the advice of the CT Infobox it is therefore the responsibility of GISS to notice that certain information is relevant for INS.

The procedure followed by INS to request GISS for information about an alien is known as a "*silent procedure*". When INS has not received a reaction from GISS within ten working days, the alien's procedure is continued without the information from GISS. The guiding principle is that such requests for information are addressed to GISS when there are signs that the service might have information relating to the alien in question. An example of such a signal is the fact that GISS has already issued an official message concerning the person in question before. Another example is that the statement made by the person concerned shows that there are links with areas of attention of GISS such as terrorism, radicalism or extremism.[60] If INS has started an investigation pursuant to Article 1F of the Convention relating to the Status of Refugees, there may also be reason to request additional information from GISS.[61]

The Committee points out that when GISS does an administrative check in its own databases at the request of INS to see whether any relevant information is available, this constitutes data processing within the meaning of the ISS Act 2002 (Article 1f ISS Act 2002). This means that such a check may only be carried out insofar as necessary for the proper implementation of the ISS Act 2002 or the Security Screening Act (Article 12(2) ISS Act 2002). Since neither the ISS Act 2002 nor the Security Screening Act contains a provision making it possible for GISS to process data for the purposes of the task of INS, the check must serve the interest of national security. If the check yields relevant data and it is decided to provide these data to INS, this must be done in the form of an official message. The legal basis for issuing official messages to INS is Article 36 ISS Act 2002. This means that the provision of data, too, must be necessary in the interest of national security.

A policy document of GISS dated 28 October 2010 concerning administrative searches and checks shows that when GISS receives a request for a check, it assesses first of all whether

[59] See for more information on the CT infobox CTIVD review report no. 12 on the Counter-Terrorism Infobox Infobox, *Parliamentary Papers II* 2006/07, 29 924, no. 16 (annex). Also available (in Dutch) at www.ctivd.nl.

[60] See the annual reports of GISS.

[61] This Article provides that persons who have committed crimes or been guilty of acts contrary to the purposes and principles of the UN are not eligible for refugee status.

such a check is consistent with the rules on the provision of data laid down in Articles 36-39 ISS Act 2002. This assessment takes account of the principles of necessity, proportionality and subsidiarity. The data is provided by means of an official message. The Committee observes with regard to this policy that the basis for the assessment that must be made before GISS proceeds to do an administrative check does not lie in the statutory provisions on data provision (Articles 36-39 ISS Act 2002), but in the general provision on data processing (Article 12 ISS Act 2002). Pursuant to Article 12 the administrative check must be necessary for the proper implementation of the ISS Act 2002 or the Security Screening Act. As was explained above, an administrative check in response to a request from INS must be necessary for the purposes of the performance by GISS of its tasks, in the interest of national security. Providing data is a subsequent step which is separate from the decision to do an administrative check. The Committee recommends that GISS correctly sets out in the applicable policy document the legal basis for doing an administrative check at the request of INS as well as the related statutory requirements.

The Committee has found that in practice the requests from INS always lead to an administrative check by the front office of GISS, which is where these requests are received. The front office conducts the check to examine whether the request can be passed on to a specific team. The team will then further deal with the request. However, this first check is also a form of data processing which should satisfy the requirement of necessity in the interest of national security. In view of this fact the Committee holds that GISS must first assess the request against this requirement before it tries to link it to a team. The assessment can be made using the form supplied by INS which among other things states the reason for the request for information.

If GISS has the intention to provide information to INS, the draft official message will be submitted to the INS liaison, so that he can assess whether the information is useful for INS and whether the text has been drafted in such a way that the message can be used in the decision-making procedure of INS. This applies to both official messages on GISS' own initiative or in response to a request from INS, and official messages in reaction to an advice from the CT Infobox. Drafts of official messages of the latter category, however, are not submitted to the INS liaison until a later stage, because the primary assessment whether the information is useful is made by the INS employees seconded to the CT infobox. The main point of the assessment by the INS liaison is to ascertain that the message content is sufficiently concrete and clear so that the conclusion of the message is not incomprehensible without further explanation. This assessment is made bearing in mind the case law of the Administrative Jurisdiction Division of the Council of State.

As regards the roles played by the team and the legal department and the approval of the official message, the procedure for making official messages to INS is identical to the procedure described in section 4.2 above. Unlike the National Public Prosecutor, however, the INS liaison does not check the accuracy of the official message against the underlying file.

5.3 Findings of the Committee

5.3.1 The number of official messages in the review period

In the review period GISS issued 46 official messages to INS. These official messages therefore account for approximately 8% of the total number of official messages. At the beginning of the review period the number of official messages issued to INS per year was significantly lower than at the end. The Committee has established that a decline set in after a peak in 2004 caused by the introduction of the CT Infobox. Since the end of 2007 the number of official messages issued to INS again rose slightly due to the fact that GISS now also issues official messages about anti-integrative behaviour.

5.3.2 Legal basis

The legal basis for the provision of data to INS is Article 36 ISS Act 2002. This Article gives rules for the external provision of data for the purpose of the proper performance by GISS of its task. Where an official message is issued in connection with the withdrawal of a residence permit or an order declaring a person who in the opinion of GISS poses a threat to national security an undesirable alien, the link with the task of GISS is obvious. Preventing the naturalisation of persons who on the basis of their radical ideas reject or call on others to reject the Dutch democratic legal order or who sympathise with violent international jihad likewise falls within the scope of the task of GISS. The Committee holds the opinion that the official messages issued by GISS to INS in the review period could rightly be based on Article 36 ISS Act 2002.

In 2009 GISS issued two official messages to INS which were aimed at enabling INS to ward off the plea of Article 3 ECHR (prohibition of torture or inhuman treatment) by the alien in question in proceedings under aliens law. In those two cases the service provided information showing that the alien in question was staying or had stayed in the country of origin of his own free will. This enabled INS to oppose the allegation that the alien feared deportation on account of the risk of torture and/or inhuman or degrading treatment.

The Committee holds the opinion that these official messages, too, could rightly be based on Article 36 ISS Act 2002. When GISS has provided data to INS which contributed to the decision to deport the alien, GISS may also contribute to the deportation decision being upheld in the proceedings under aliens law by providing relevant further information. In such a case it is of course important that either the data in question had already been collected previously, or that for the purpose of the task of GISS there is reason to perform investigative acts yielding such further information.

5.3.3 Content

The Committee's investigation has shown that all but one of the official messages issued by GISS to INS in the review period (see section 5.3.4) are substantiated by the underlying information. The messages are, moreover, carefully formulated, so that they are in line with the underlying information.

The Committee has found that GISS does not use a consistent definition of the term "threat to national security". GISS considers on a case-by-case basis whether this conclusion applies. Each of the official messages examined by the Committee concerned activities having such a clear connection with national security, that in the opinion of the Committee they justified the conclusion. The activities consisted of actively supporting and/or participating in violent international jihad or participating in a terrorist organisation.

It emerged in section 5.1 that official messages to INS must contain sufficiently concrete and specific information to give the alien elements for his defence. In addition, GISS must take account of the fact that INS will not be permitted to simply base its decisions on the official message without inspecting the underlying documents if the text of the message does not show on which facts and circumstances its conclusion is based. In 2009 and 2010 GISS issued three official messages supplementary to official messages it had issued earlier. They concerned three separate cases in which INS had requested GISS to provide further factual information. In line with the judgment of the ECtHR in *A. e.a.* v. *United Kingdom*[62] the supplementary official messages stated, as far as was possible for reasons of source protection and keeping secret the current level of knowledge and/or the operational methods of the service, with which persons contacts were maintained and when these contacts took place. A judgment of the District Court of The Hague of 26 January 2010 shows that such an approach may lead to the decision-process being upheld.[63] However, the Committee draws the attention of GISS to the fact that it is important for the alien about whom the service issues an official message that he receives sufficient factual information at the earliest possible stage. When the protection of sources, the secrecy of the current level of knowledge and/or the operational methods of the service or the third party rule[64] do not constitute a reason to withhold concrete details, then in the opinion of the Committee GISS should therefore seek to provide INS with as much concrete information as possible.

5.3.4 Indication of reliability or source reference

The Committee has established that the official messages issued by GISS to INS contain an indication of reliability.

In one case the Committee has established that with respect to part of the information provided the indication of reliability in the official message was not substantiated by the underlying file. In this official message, issued 2006, it was stated that the information "was obtained from a reliable source". The underlying information, which had been provided by the Regional Intelligence Service, did not include an indication of the source or its reliability. It emerged from the Committee's investigation that the reliability of the information from the Regional Intelligence Service had not been established. The Committee points out that the indication of reliability, like the rest of the text of the official message, must find support in the information in the possession of GISS. When it is not fully supported thereby, as in this particular case, the official message cannot be said to have been drafted with proper and due care. In this respect the official message is unlawful. The Committee therefore recommends that GISS records this in the relevant file pursuant to Article 43(2) ISS Act 2002 and informs INS that the reliability of the sources on which the first part of the official message is based has not been established.

---

[62] ECtHR 19 February 2009 (*A. a.o.* v. *United Kingdom*), A 3455/05, para. 220.
[63] District Court of The Hague 26 January 2010, *LJN*: BL0575.
[64] Foreign services often provide information subject to the condition that it may only be passed on if the foreign service in question has granted permission to do so. See for a more detailed discussion of this subject review report no. 22a of the Committee on the cooperation of GISS with foreign intelligence and/or security services, *Parliamentary Papers II* 2009/10, 29 924, no. 39 (annex). Also available at www.ctivd.nl.

As a result of the above case the Committee investigated more closely how the Regional Intelligence Services provide information to GISS pursuant to Article 60 ISS Act 2002 and whether in doing so they comply with Article 12(4) ISS Act 2002 as well. The notification forms used by the Regional Intelligence Services usually have a separate line for evaluating the reliability of the source. The Committee has found that this item is often not filled out. Where it is filled out, the reliability indication is ambiguous, since the Services use different coding systems and qualifications. This way of processing information is contrary to Article 12(4) ISS Act 2002. The Committee recommends introducing clear and unambiguous indications of the reliability of information passed on by Regional Intelligence Services to GISS.

6 Official messages to the ministry of Economic Affairs, Agriculture and Innovation

6.1 Use of official messages to the ministry of Economic Affairs, Agriculture and Innovation ("EAA&I")

The ministry of EAA&I is responsible for the export controls of strategic goods, including so-called dual-use goods. These goods are suitable for both civil and military use. Dual-use goods are often considered to be strategic goods because of the fact that they can be used to manufacture WMD.

The most important instrument for controlling the export of strategic goods is the licensing system. Formally, decisions on applications for export licences are taken by the Central Import and Export Office which falls under the customs and therefore under the ministry of Finance. When granting or refusing applications for export licences for strategic goods, however, the Central Import and Export Office acts on the instructions and under the responsibility of the minister of EAA&I. With respect to applications for exports to non-sensitive destinations, such as allies of the Netherlands, the Office has been authorized to deal with the applications independently. All other applications, including applications for exports to so-called countries of concern, are dealt with as regards content by the ministry of EAA&I. For various reasons, exports to these countries require special controls. When an application for the export of dual-use goods concerns export to a country of concern, the ministry of EAA&I will as a rule obtain information from the joint counter-proliferation team of GISS and DISS, the Counter Proliferation Unit.

When GISS provides information to the ministry of EAA&I for this purpose, this is considered an official message because the information is provided to a body which is authorised to act on the information by taking measures. This is so because information from GISS may result in refusal of an export application or the ad hoc imposition of an obligation to obtain a licence. It is true that these official messages come from the joint GISS and DISS unit, but they fall under the responsibility of the head of GISS. The official messages to the ministry of EAA&I are issued in the context of the task of GISS based on Article 36 ISS Act 2002.

The current arrangement between GISS and the ministry of EAA&I is that GISS indicates whether information is available which shows that the final customer or a middleman has ties with proliferation-relevant and/or military-sensitive projects. The official message may also provide information about whether the goods in question can be used in WMD

programmes or for making means of delivery (e.g. cruise missiles). Based on an oral arrangement with the ministry of EAA&I, GISS expresses an opinion on the usability of the goods if it is expressly requested to do so. The legislature has vested the ultimate assessment of all the interests involved in the ministry of EAA&I .[65] In its decision-making process the ministry devotes attention to the exporter, the end-user and the middleman, the goods and their stated end-use and also the risk that the goods will be put to a different end-use. Refused licence applications are periodically discussed at the interministerial committee on exports of strategic goods, of which GISS is a member.

The Committee has found that GISS has started consultations with the ministry of EAA&I about laying down the arrangements in the field of information provision in a covenant. The Committee endorses the usefulness of such a covenant.

In addition to the official message issued in response to requests from the ministry of EAA&I it also happens that GISS issues an official message to the ministry of EAA&I when indications have emerged during an investigation that a person or company is circumventing the rules applying to the export of strategic goods. Such an official message may result in an inspection visit to the company or the imposition of an ad hoc obligation to obtain a licence.

Unlike the Public Prosecution Service and INS (on request), the ministry of EAA&I is not granted inspection of the files underlying the official messages. Pursuant to Article 40(3) ISS Act 2002, the minister of the Interior or the head of GISS on his behalf may decide to grant a person or an agency inspection of the information underlying the official message to the extent necessary to assess the accuracy of the message. So far, this option has not been used yet in respect of official messages to the ministry of EAA&I.

Decisions of the ministry of EAA&I on applications for an export licence for strategic goods are open to objection and appeal. Appeal lies to the Trade and Industry Appeals Tribunal (Article 13(1) Import and Export Act). When the ministry of EAA&I decides to impose an ad hoc obligation to obtain a licence, the party concerned can lodge an objection to this decision with the ministry and file an appeal with the administrative courts. In such proceedings against a decision based among other things on information from GISS, the ministry of EAA&I may have to submit the official message from GISS to the administrative court in order to substantiate a decision. In that case the rules of Article 8:29 of the Dutch General Administrative Law Act ("GALA") are followed, which provide that the court is informed that the document will only be disclosed to the court. The reason for this is that the official messages issued by GISS to the ministry of EAA&I for the purposes of the supervision of exports are classified state-secret. If the court decides that the restriction on disclosure is justified, the other party (the exporter) will also have to consent to the court partially basing its judgment on the official message (Article 8:29(5) GALA).

6.2 Procedure for making official messages to the ministry of Economic Affairs, Agriculture and Innovation

If an application for an export licence is submitted to GISS, the ministry of EAA&I submits the entire file containing the licence application, the underlying technical documentation and

[65] Strategic Goods Decree, *Stb*. 2008, 252, Article 3(1.

the preliminary report of the Central Import and Export Office[66]. Upon receiving the file, the Counter Proliferation Unit first examines whether any relevant information on the end-user and/or middleman concerned can be found in the databases of GISS and DISS. In certain cases the Unit will submit a request for information to foreign counterparts of GISS.

Generally, no preliminary consultations take place between the recipient body and GISS concerning official messages to the ministry of EAA&I, thus making the procedure different from the one applying to official messages to the Public Prosecution Services and INS. There are, however, periodical bilateral consultations concerning official messages in a general sense. For example, the parties discuss the use of certain standard phrases and terms. In principle, the Counter Proliferation Unit does not provide oral information on the substance of specific official messages, because ultimately the ministry can only base its decisions on information it has received in writing. Questions serving to elucidate official messages already issued may, however, be answered.

Just like the official messages to other recipients, official messages to the ministry of EAA&I are successively approved by the team head, the legal department, the unit head and finally the management of GISS.

6.3 Findings of the Committee

6.3.1 The number of official messages issued in the review period

Because GISS plays a standard role in the procedure for assessing licence applications for exports of dual-use goods to countries of concern, the annual number of official messages issued to the ministry of EAA&I is high. In the review period GISS issued 340 official messages to the ministry of EAA&I; about 60% of the total number.

6.3.2 Classification

The official messages issued by GISS to the ministry of EAA&I differ from other types of official messages because they are classified state-secret and for this reason cannot be provided to the person or company concerned. This is not consistent with the basic principle emerging from the Explanatory Memorandum to the bill containing the ISS Act 2002 (underlining by the Committee):

> "If it is expected that the competent authority will, on the basis of the information to be provided, take measures against the person concerned which may prejudice his legitimate interests, the information shall be provided by means of a written (unclassified) official message."

A footnote to the Explanatory Memorandum states that the term unclassified official message means an official message that is drafted in such a way that the person to whom the

[66] The Central Import and Export Office issues a preliminary report that is based on administrative checks in a number of databases and on information supplied by the exporter.

official message relates can without any objection take note of its content. The Explanatory Memorandum puts forward two reasons for the principle:

> "On the one hand it creates the possibility for the agency concerned to take the measures with due care and substantiated by reasons and on the other hand the procedure makes it possible for the person concerned to defend himself in court."

The interviews conducted by the Committee with employees of GISS showed that GISS takes the position that the main reason for classifying the official messages lies in what these messages reveal about the current level of knowledge at GISS. The messages indicate what is the information position of GISS with respect to specific end-users and/or middlemen in the intended countries of destination of the goods. Evilly-disposed persons having this knowledge might adjust their licence application, e.g. by stating different end-users. Usually, moreover, the information in question originates from ongoing investigations of GISS. Another factor that plays a role, so GISS stated, is that these official messages are often based on information from foreign counterpart services to which the third party rule applies.

The Committee observes in this context that the considerations mentioned by GISS apply to a certain extent to all official messages issued by GISS. Balancing interests, the service has decided to disclose its current level of knowledge concerning a specific person or organisation so that measures can be taken. The idea is that the measures will eliminate or reduce the threat emanating from the subject under investigation, so that it will perhaps no longer be necessary to conduct further investigations (at any rate of that specific person or organisation. This does not hold good in the case of official messages for the purpose of export applications. These official messages state in particular to what extent certain companies in foreign countries can be associated with the proliferation of WMD. It is not possible, however, to take measures against these companies, because they are established abroad. If an attempt to acquire goods is foiled, the threat emanating from these companies will not decrease. In this situation national security is best served by secretly identifying the attempts of these companies to acquire certain goods and by preventing the Netherlands from making a contribution to proliferation by enabling the ministry of EAA&I to refuse the licence applications concerned. If the information position of GISS regarding companies in certain countries becomes public knowledge, the possibility of monitoring their actions disappears. The Committee holds the opinion that in those cases the general interest of national security must carry greater weight than the individual interest of the exporter in learning the content the official message. Taking into consideration that the information provided to the ministry of EAA&I in connection with export applications will by definition reveal nature be traced to the current level of knowledge of GISS regarding companies in countries of concern, the Committee holds the opinion that the classification of these official messages is justified.

This opinion of the Committee is supported by a recent judgment of the District Court of Haarlem.[67] The exporter in this case had lodged an appeal against the fact that he had not been permitted to learn the content of the official messages from GISS that formed the basis of nine refusals of licence applications. The District Court ruled that restricted disclosure of the official messages was justified in the interest of keeping secret the current level of knowledge, the sources and the operational methods of GISS. Of decisive importance was the consideration that if the official messages were to be disclosed, the risk that the

[67] District Court Haarlem 14 September 2010, AWB 10/2199, 10/3929, 10/3930, 10/3932, 10/3933. 10/3934, 10/3979 and 10/3990.

implementation and enforcement of legislative and other rules would be frustrated might materialise. Based on the information stated in the official messaged other exporters would be able to develop a method to circumvent the aforementioned legislative and other rules, in particular the restrictions on exports to Iran.

Although the Committee holds the opinion that the classification of the official messages is justified, it points out that the state-secret nature of the messages does not only have disadvantages for the exporter concerned, but also for the ministry of EAA&I which has based its decisions on secret information. If administrative proceedings should ensue, then because of the agreements made on the subject between GISS and the ministry of EAA&I it is for GISS to decide whether an official message may be disclosed to the court. If GISS decides that the official message may not be submitted in evidence, for example because of the third party rule, the court may draw such conclusions from this fact as it deems appropriate (Article (8:31 GALA). This might have the result that the decision of the ministry of EAA&I is reversed.

The problem discussed above can be illustrated with an example from the Committee's investigation. In 2006 and 2007 GISS, in response to export applications filed by a company, issued official messages to the ministry of EAA&I providing information on the ties of the named end-user with a nuclear programme. On the basis of this information the ministry of EAA&I imposed ad hoc licensing obligations on the company for certain types of goods. The company filed objections with the ministry, lodged an appeal with the district court and subsequently appealed to the Court of Appeal. For the purposes of the proceedings before the Court of Appeal the ministry of EAA&I asked GISS for permission to submit the information provided by GISS at an earlier stage to the Court of Appeal, in order to give insight into the substantiation of the decisions. In reply to the request GISS communicated that it preferred issuing a new official message instead of permitting the ministry to submit the earlier official messages in evidence. But the new official message that was issued for submission in the appeal proceedings contained less specific information than the earlier official messages. This posed a potential problem for the ministry of EAA&I in the proceedings, since it was not permitted to submit the information on which the challenged decisions were based. In this situation the ministry of EAA&I had no choice but to wait and see whether the appeal court would find that the new, more cautiously drafted official message also constituted a sufficient basis for the decision. In this particular case the exporter withdrew the appeal to the Court of Appeal, so that the court did not give a decision on the issue.

The Committee has found that GISS' decision in this case to provide less specific information to the ministry of EAA&I for the purposes of the appeal proceedings was connected with an ongoing investigation of the service. For operational reasons GISS considered it too great a risk to allow the earlier official messages to be submitted in evidence to the Court of Appeal. The Committee appreciates the arguments of GISS, but it holds nevertheless that it is not right that the ministry of EAA&I was entirely dependent on GISS in the matter. When classified information is disclosed to a third party for use in the decision-making process of an administrative body, then from the perspective of GISS there is no reason not to disclose this information to the courts, subject to secrecy. If the information is highly sensitive with a view to source protection and keeping secret the current level of knowledge and/or the operational methods of the service or if it has to observe the third party rule, these are reasons for not disclosing the information to the ministry of EAA&I. The Committee holds the opinion that once this step has been taken, GISS can hardly deprive the ministry of

EAA&I of the possibility to substantiate its decision by submitting the official message to the court.

Now that the exporter cannot be given the possibility of learning the content of the official message and as a result is not in a position to question the statements of GISS, this emphasizes the importance of careful decision-making by the ministry of EAA&I. For this purpose the ministry of EAA&I must have sufficient factual information at its disposal. Because standard phrases are used that give a general description of the underlying information, the text of these official messages does not furnish a great deal of factual information (see on this issue section 6.3.3.1). Moreover, the ministry of EAA&I is not granted inspection of the documents underlying the official messages, in spite of the fact that GISS' contact at the ministry has A-level screening. The Committee draws attention to what the Explanatory Memorandum to the ISS Act 2002 stated about inspection of the documents underlying official messages:

> "Where a measure has far-reaching consequences for the party concerned and the decision-making authority has little or no other incriminating material in its possession, the competent authority will as a rule be given the opportunity, subject to secrecy, to inspect the information constituting the basis of the official message that has been issued. This serves the purpose of enabling the authority, acting as a careful administrative body, to make sure that the facts are supported by the underlying information which must be kept secret, for example for reasons of source protection."[68]

The regular bilateral consultations between GISS and the ministry of EAA&I about official messages generally, and sending intelligence reports in order to furnish certain background information are steps in the right direction, but in the opinion of the Committee they do not sufficiently overcome the problem of the ministry's limited information position. The Committee therefore recommends that GISS, in consultation with the ministry of EAA&I, seeks ways to promote that the ministry can make its decisions on the basis of an adequate information position. One possibility is that of granting the ministry of EAA&I, where necessary, inspection of the documents underlying the official messages.

6.3.3 Content

6.3.3.1 The use of standard phrases and terms

Since GISS issues many official messages to the ministry of EAA&I per year, it is increasingly using standards phrases in the official messages. In the summer of 2010 the ministry of EAA&I, in consultation with the Counter Proliferation Unit, prepared a matrix setting out how the information received from GISS will be reproduced in the decision to be received by the exporter. This 'translation' is necessary because of the classified nature of the official messages. The matrix mentions four categories of ties with proliferation-sensitive projects in the order of increasing seriousness:

1) no ties with proliferation-sensitive projects;
2) end-user/middleman is an entity of concern;

[68] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 55.

3) end-user/middleman has no direct ties or has indirect ties with proliferation-sensitive projects;
4) end-user/middleman has ties with proliferation-sensitive projects.

The Committee has established that in the past particularly the category "no direct ties" was not always applied consistently. GISS informed the Committee that this category is used when it has not been established that the middleman/end-user himself has ties with sensitive projects, but that he can be related to another company that has ties with sensitive projects. Although the matrix that has been prepared is primarily intended as a guideline for the ministry of EAA&I in its communications with exporters, the Committee expects that it will promote consistency in the official messages. The formalisation of the 'translation' of the different standard phrases has produced clarity.

The Committee points out, however, that the use of standard phrases having a fixed meaning entails the danger that certain qualifications disappear from the messages. It further observes that the chosen wordings have a low factual content. Where it is stated, for example, that a specific end-user/middleman has ties with proliferation-sensitive projects (further referred to as: sensitive projects), this does not show the exact nature of the ties. The Committee has found that general descriptions were chosen because in many cases the underlying information originated from foreign counterpart services. On account of the third party rule, the Counter Proliferation Unit usually does not have the option of passing on the information it has obtained, while it does consider it necessary to do so to give the ministry of EAA&I a signal for the purposes of its decision-making.

The Committee considers it important that GISS assesses for each official message separately whether the chosen standard phrase adequately represents the underlying information and whether it is possible to provide more factual information than the standard phrase without affecting the agreements made with foreign counterpart services and the secrecy of sources, current level of knowledge and/or the service's operating procedure.

A frequent closing sentence of the official messages to the ministry of EAA&I is that it cannot be excluded that the goods will be used in sensitive projects. The Committee has noticed that this sentence is used inconsistently in the official messages issued to the ministry of EAA&I in the review period. When asked about this, GISS stated that there was no clarity as to when the sentence could be used. For this reason GISS had decided that it would no longer include the sentence in official messages in the future. The Committee agrees with this decision, since the sentence does not add any substantial information while the ministry of EAA&I did in fact interpret it as an aggravating note in the official messages.

As a result of the standardised nature of the official messages issued by GISS to the ministry of EAA&I, certain expressions keep recurring. This is understandable, but it entails the risk that certain matters are ranged under a common denominator which is not fully applicable in all cases. A frequently used expression in these official messages is "associated with". The Committee has found that this expression may refer to several types of connections. It can mean, for example, that there are commercial family or ownership connections. The expression is also used when the end-user/middleman in a certain project is the party that awarded a contract to another company. The Committee holds the opinion that where a company has merely awarded a contract in a certain project, this cannot be said to imply a lasting relationship. It holds that the expression "associated with" is not a correct description of temporary collaboration. The Committee considers it important that henceforth GISS

chooses a description that is as closely as possible in keeping with the underlying information.

6.3.3.2 Substantiation

In the course of its investigation the Committee had a number of interviews with employees of GISS about the official messages issued to the ministry of EAA&I. During these interviews attention was paid to the nature of the messages. Initially, the discussion was about whether or not this form of providing information must be considered official messages. As was explained in section 6.1 above, the Committee holds the opinion – and by now GISS also does so – that the messages must indeed be considered official messages, since they provide information to an authority which is authorised to take measures. Precisely because official messages may lead to measures being taken, it is important that the information provided is substantiated by the underlying file.

It has emerged from the Committee's investigation that GISS, which formerly did not consider the messages to the ministry of EAA&I to be official messages, did not always set very high requirements on the substantiation of the messages. The Committee will now discuss two cases in which the underlying information proved to be insufficient basis for the message.

In the first case, an official message issued in 2008, the ministry of EAA&I was informed that the end-user had connections with sensitive projects. Upon examining the file the Committee found that this allegation was based on a refusal of an application for an export licence by another country. In a European context and also in the context of certain multilateral forums, such refusals (further called "denials") are exchanged.[69] The reason stated for the denial was that there was an unacceptable risk of diversion to a ballistic missile programme. The Committee considered this denial to constitute insufficient substantiation for the allegation that the end-user had connections with sensitive projects. Apart from the end-user, the nature of the goods may also play an important role in the context of such denials. Since the aforementioned denial related to a different type of goods, the Committee deems it possible that the nature of the goods played a role in the decision-making of the country in question. Without making inquiries at the authorities of this country, GISS should not have concluded from the denial that the end-user had connections with sensitive projects. The Committee therefore holds the opinion that the official message in question is not substantiated by the underlying information. The official message was not drafted with proper and due care and is therefore unlawful.

The second example of an official message which in the Committee's opinion is not substantiated by the underlying information is another message issued in 2008. The conclusion that the end-user had ties with sensitive projects was substantiated by a message from a foreign counterpart service. The information from the counterpart service only showed that the end-user was included in the watchlist[70] of the country in question and that

[69] The policy within Europe is that such a denial in one country constitutes reason for other countries not to grant export licences either in the case of similar transactions. Similar transaction in this context means: the same product, or a product having sufficiently similar technical characteristics, and also the same intended end-user.

[70] Some countries compile a so-called *watchlis*t of companies which for various reasons are labelled "entity of concern". Such a list contains e.g. the end-users that have been reason for the country in

a denial had been issued in the past with respect to the end-user. The reason stated for the denial was the risk that the goods would be used to manufacture equipment which might be deployed against the armed forces of European Member States or their allies. In addition, the denial stated that there was a risk that the goods would be diverted within the country of destination or would be re-exported under undesirable circumstances. In the opinion of the Committee the information provided by the counterpart service does not show that the end-user actually had ties with sensitive projects. Since the further information in the file cannot substantiate the said ties with sensitive projects either, this official message, too, is not adequately substantiated. In the Committee's opinion, therefore, this official message is unlawful as well.

The Committee recommends that GISS, pursuant to Article 43(2) ISS Act 2002, makes a record of this fact in the relevant file and informs the ministry of EAA&I, with a view to possible future applications for export licences for the benefit of the end-users concerned, that the two aforementioned official messages are not substantiated by the information in the possession of the service.

6.3.4 Mention of denials

It emerged in section 6.2 that the Central Import and Export Office issues a preliminary report based on administrative checks in a number of databases before the file is sent to GISS. One of these databases is the database compiled at European level and containing all denials of the Member States. The exchanged denials from other regimes such as the Australia Group[71] and the Missile Technology Control Regime (MTCR)[72] are also included in this database. In addition to the Central Import and Export Office, the ministry of EAA&I and GISS also have access to this database. The Committee has established that it frequently happens that GISS mentions denials in the official messages. In 2010 it was agreed that GISS would only mention denials if the preliminary report of the Central Import and Export Office shows that it has not found the denials in question while they are in fact registered in the system.

The Committee observes here that double checking may have the result that ultimately neither party checks the information really carefully, because each party assumes that the other party has already done so. It should be clear who is responsible for consulting the database. The Committee was told by GISS that early in 2011 it was arranged with the ministry of EAA&I that the responsibility for checking the database would rest with this ministry.[73] Consequently, GISS will no longer mention denials in the official messages.

---

question to deny an export licence. Watchlists are usually accessible to the public so that exporters can consult them.

[71] The Australia Group is an international forum within which non-binding rules have been drawn up for the export of certain 'sensitive' goods which rules are intended to prevent the proliferation of chemical and biological weapons. See also: www.australiagroup.net.

[72] The goal of the Missile Technology Control Regime is to prevent the proliferation of weapons of mass destruction by controls on the export of delivery systems for weapons of mass destruction (other than manned aircraft). Non-binding rules have been drawn up for this purpose. See also: www.mtcr.info.

[73] Although this arrangement falls outside the review period, the Committee mentions it for the sake of completeness.

6.3.5 Indication of reliability or source reference

The Committee has found that the official messages issued by GISS to the ministry of EAA&I in the early part of the review period usually do not contain an indication of reliability. This means that in this period GISS did not comply with the statutory requirement of Article 12(4) ISS Act 2002. From early in 2009 GISS has included an indication of reliability in the official messages, with the result that the ministry of EAA&I now obtains an understanding of the quality of the information on which its decision-making is based.

It is the opinion of the Committee that the fact that in the earlier period the messages to the ministry of EAA&I were not considered official messages is not an adequate explanation for omitting to include an indication of reliability in the messages over a long period. The statutory requirement that data processed by GISS must be accompanied by an indication of reliability or source reference applies not only to official messages, but to all forms of data processing for the purposes of the performance by the service of its tasks. Consequently, this requirement would also have applied if the messages to the ministry of EAA&I had been advisory letters, as GISS used to think. Moreover, GISS knew that the ministry of EAA&I would include the information provided by GISS in its decision-making process, so that it should have been clear that an indication of its reliability was necessary for the ministry to be able to assess the value of the information.

Meanwhile, GISS has made arrangements with the ministry of EAA&I about how the reliability of information from various types of sources is assessed and how this is represented in the official messages. In March 2010 these arrangements have been formalised in a policy document which is applied consistently, so the official messages examined by the Committee show.

Pursuant to this policy document, information from public sources, for example the Internet, is represented in official messages as follows: *"from a publicly accessible source …"*. The interviews held by the Committee in the course of its investigation have shown that both the ministry of EAA&I and GISS collect information about end-users/middlemen from publicly accessible sources. At the ministry of EAA&I this is done during the stage following the despatch of the file to GISS. When GISS reports to the ministry of EAA&I that certain information on the end-user/middleman has emerged from a publicly accessible source, it may happen that it is not clear to the employees at the ministry whether this is the same information they had already found themselves. Although it is possible that the ministry of EAA&I will consult with GISS in case of doubt, the Committee fails to see why GISS does not mention the specific public source of information in the official messages, so that no misunderstandings can arise on this point. Transparency should be pursued wherever possible, certainly in the context of a task – in this case the collection of information from publicly accessible source – which is performed by two agencies.

As a result of recent interviews with the Committee, this point was the subject of internal consultations at GISS. It was decided that GISS will henceforth mention the specific source of the public information it has found.

Information from human sources is seldom used in official messages to the ministry of EAA&I. The Committee has established that the Counter Proliferation Unit, unlike the other departments of GISS, does not prepare reliability memorandums for the underlying file in such cases. This is not in keeping with general policy at GISS in this area. The Committee recommends that the Counter Proliferation Unit adjusts its procedure.

6.3.6 Requirements applying to the provision of personal data

By far the largest part of the official messages issued by GISS to the ministry of EAA&I relate to companies in the countries of destination of the goods. It is open to discussion whether the statutory provisions that are applicable to the external provision of personal data are also applicable to these official messages. The definition of personal data in the ISS Act 2002 is (virtually) identical to the definition in the Personal Data Protection Act:[74]

> "information relating to an identifiable or identified, individual natural person" (Article 1(e) ISS Act 2002)

When deciding this issue the Committee therefore followed the explanation given to this provision in the Personal Data Protection Act. The Guide for persons who process personal data, drawn up by the ministry of Justice, shows that as a rule data on enterprises are not personal data. Exceptions are only made for certain data on one-man businesses which can be traced directly to the owner of the business. The Committee therefore holds the opinion that the data provided by GISS to the ministry of EAA&I is not personal data.

Nevertheless, the Committee finds that where data is provided which may result in measures being taken against persons or companies, the same proper and due care must be exercised as in the case of the provision of personal data. An official message to the ministry of EAA&I may, for example result in denial of an export licence, which is a measure which, though not directed against the middleman or end-user with respect to whom data have been provided, may yet have far-reaching consequences for the applicant. Because of the potential consequences of the provision of such data the Committee considers it appropriate that the special requirements of proper and due care mentioned in Articles 40, 41 and 42 IIS Act 2002 apply to the official messages to the ministry of EAA&I.

One of the safeguards ensuring that personal data will be provided with proper and due care is the provision that personal data may not be provided if it cannot in reason be established that the data is accurate or if the data has been processed more than ten years ago and no new data has been collected regarding the person since then (Article 41(1) ISS Act 2002). According to the policy in place at the Counter Proliferation Unit, information used in official messages to the ministry of EAA&I must not be older than ten years. However, the information can also prove out-of date before then, for example if the situation in the country in question has changed dramatically. When the information is so incriminating that it really cannot be disregarded, the service may decide to include information older than ten years nevertheless. The Committee has established that the Counter Proliferation Unit applies these guidelines.

The Committee holds the opinion that this policy satisfies the requirements of due care to a sufficient degree. By analogy with Article 41(3) ISS Act 2002, however, the degree of reliability and the age of the data must be mentioned if the data on which the official message or part of the official message is based is older than ten years.

---

[74] Conceptually, the ISS Act 2002, where relevant, follows the Personal Data Protection Act. (*Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 17).

In one case GISS issued an official message to the ministry of EAA&I containing information which dated back twelve years. The Committee points out that if this information was deemed so incriminating that it could not be disregarded, the official message should in any case have mentioned the degree of reliability and the age of this information, which did not happen in this case. The Committee considers this to be negligent.

Another requirement of due care which is appropriate in the case of the official messages to the ministry of EAA&I, given their purpose and the interests at stake, is the requirement that the information must be provided in writing. The Counter Proliferation Unit does indeed have a rule that all (specific) data provision to the ministry of EAA&I takes place in writing. The Committee has found that this rule is usually observed meticulously at the Counter Proliferation Unit. In two cases, however, the Committee has established derogation from this policy. In both cases the Counter Proliferation Unit had relevant information which – on the basis of the policy outlined above – was found too old to be provided to the ministry of EAA&I. The information was indeed not incorporated in the official messages that were issued. Oral information was, however, communicated from the Counter Proliferation Unit to the ministry of EAA&I that 'something' had been found. The exact content of these communications can no longer be retrieved. The Committee considers that the Counter Proliferation Unit has acted with due care in both cases by not wishing to include the outdated information in the official messages. It points out to GISS, however, that a communication that something has been found, without any indication of what the information consists of, can also influence the decision-making process. The Committee holds the opinion that for reasons of due care the service must refrain from making such remarks in its contacts with the ministry of EAA&I.

6.3.7 Documentation

In the past few years the files of the official messages to the ministry of EAA&I have distinctly gained in clarity. Although formerly, too, the files always included a so-called "investigation export form", on which it was recorded which investigative actions had been performed in response to the request from the ministry of EAA&I and certain documents from the underlying file were named, it was nevertheless not always easy to understand the underlying file, which was often fairly technical in nature. Early in 2009 the Counter Proliferation Unit started adding an annotated version of the official message to the underlying file, in which it stated the document numbers of the underlying documents supporting the information in the official message. In the opinion of the Committee this is a great improvement, since now it is immediately clear how the underlying documents have been used.

Sometimes, only the relevant pages of large documents are included in the files of the official messages issued to the ministry of EAA&I, or it is otherwise impossible to retrieve from which document the pages are taken. The Committee recommends that in such cases the Counter Proliferation Unit indicates what is the document concerned and mentions its date.

7 Official messages to political party chairpersons

7.1 Background and policy

In 1993 the media brought the news that members of organised crime had attempted to infiltrate politics by nominating candidates for municipal elections. In reaction to the news a discussion flared up in the Second Chamber about countering such attempts.[75] In this context the Second Chamber also discussed the role of the National Security Service (BVD), which had issued official messages regarding the political candidates to the political parties for which they were candidates. The minister of the Interior explained to the Second Chamber that the National Security Service had issued official messages to the parties themselves, because ultimately the party is the entity which the person concerned can call to account if consequences are attached to the information. The minister stated that four considerations play a role in deciding to provide incriminating information:

1. the importance of the position which the person concerned has or wishes to acquire in relation to politics;
2. the position of the person concerned relative to organised crime;
3. the question whether this fact could also become known without the interference of the National Security Service;
4. the question how the issue relates to the fundamental rights of the person concerned, such as his right to be elected and the right to be able to defend himself.

Summarising, the minister stated that the matter called for restraint and that the prime consideration should be the self-correcting capacity of politics. The National Security Service could only have a task in the matter if the facts and circumstances gave reason for serious suspicions and the party concerned could not itself become aware of them.

The basic principles of a political party's own responsibility and of subsidiarity described by the minister of the Interior were maintained in the agreements made in 1997 with the political parties. In May 1998 these agreements were laid down in the Memorandum "The National Security Service and integrity risks with respect to (candidate) political office holders".[76] The Memorandum outlines the procedure for dealing with a request for information from a party . The Memorandum states first of all that the National Security Service does not do security screenings of political office holders, because political offices cannot be considered to be offices of confidentiality.

The 1998 Memorandum provides that the National Security Service will provide information in two situations:

---

[75] *Proceedings II*, 17 February 1994, 52, 3974-3975.

[76] The term political office holders means: aldermen and members of the provincial executive, mayors and Queen's commissioners and people's representatives at the central and decentralized levels and representatives in the European Parliament. See also *Parliamentary Papers II* 2005/06, 28 479, no. 26, p. 1.

1. At the request of a political party the National Security Service has investigated a person who is suspected to pose a threat to the integrity of the public sector;
2. In the context of its ongoing performance of its tasks the National Security Service has come across a (candidate) political office holder who may pose a threat to the integrity of the public sector.

With regard to investigations by the National Security Service at the request of a political party, the Memorandum states that the National Security Service may only comply with such a request after the party has itself used all possibilities to investigate misgivings. For this purpose the party can ask the person concerned to submit a detailed resume, a statement of other positions he is holding and a certificate of good character. Furthermore, the party can hear informers and references about the person concerned. If after using the aforementioned means there is or continues to be a suspicion that the person concerned poses a threat to the integrity of the public sector in some form or other, then the National Security Service may investigate the person. Having regard to the principle of proportionality the National Security Service must, in doing so, take account of the seriousness of the suspicion and the gravity of the threatening impairment of the integrity of the public sector.

In October 2006 a new policy memorandum was drafted, on the basis of the ISS Act 2002, concerning GISS and integrity risks relating to (candidate) political office holders (further referred to as: the policy memorandum). This policy memorandum was sent to the political party chairpersons. As in the earlier version, the own responsibility of the political parties and the principle of subsidiarity are the guiding principles of the policy. Pursuant to the memorandum GISS may only be called in if, after using all means available to a party, a suspicion exists or continues to exist that a (candidate) political office holder poses a threat to the integrity of the public sector in some form or other. The greatest substantive difference with the earlier memorandum is that the new policy distinguishes between conducting an administrative check and conducting an investigation. The memorandum states that if a request from a political party gives reason to any action on the part of GISS, the first action will consist of doing an administrative check in the service's own databases. If the result of the administrative check, in combination with the information provided by the political party, gives rise to the serious suspicion that the (candidate) political office holder poses a threat to the democratic legal order, national security or other vital state interests, then GISS can conduct an investigation based on its task under (a). As regards legal basis, the policy memorandum places doing an administrative check in the same category as providing information (Article 36 ISS Act 2002).

In September 2010 GISS revised the policy memorandum and sent it the chairpersons of the political parties in the Second Chamber. The most recent version of the policy memorandum is directed at candidate members of parliament, instead of the wider group of (candidate) political office holders. The reason stated by GISS for this adjustment is that in recent practice the rules had been applied only to candidate members of parliament. Another change is that the new version states more emphatically that it is the responsibility of the political parties to investigate the integrity of (candidate) political office holders.[77] In addition, it has now become an element of the procedure that the Committee is informed whenever information

[77] The policy memorandum of 2006 states that it is "advisable to a high degree" that the parties investigate misgivings themselves. The recent version states that political parties are themselves responsible for ascertaining that the political office holders of their party do not pose a risk for the integrity of the public administration.

is provided on a (candidate) political office holder. For the rest the text drafted in 2006 has been maintained.

The Committee holds that the provision of information on a (candidate) political office holder to a party chairperson in response to a request or on the own initiative of GISS is an official message, since the information is provided to the body that is authorised to take measures as a result of the information, for example withdrawing or replacing a candidate for a specific political office.

The policy memorandum defines an administrative check as a form of providing information pursuant to Article 36 ISS Act 2002. As was already discussed in section 5.2, the Committee considers this definition to be incorrect. Pursuant to Article 1(f) ISS Act 2002, consulting and/or compiling data falls under the term data processing. GISS has power to do this pursuant to Article 12(1) ISS Act 2002. Providing data is another form of data processing on which the law imposes special requirements (Articles 36-42 ISS Act 2002). Every act of data processing by GISS must in itself be necessary for the proper implementation of the ISS Act 2002 or the Security Screening Act (Article 12(2) ISS Act 2002). The legislative history shows that this provision means that the service may process data either for the purpose of the performance by the service of its tasks, or for the purpose of the statutory activities of the service falling outside the performance by the service of its tasks (see section 3.1.1). GISS may only do an administrative check in reaction to a request for information from a party chairperson in the context of its statutory tasks. This must be assessed directly; the objective of the administrative check must form part of the performance of the statutory tasks under Article 6(2) ISS Act 2002. In the absence of a legal basis for processing or providing data for the purpose of the tasks of the party chairpersons, providing data to party chairpersons cannot be a separate purpose of the administrative check.

As was stated in section 3.1 of this review report, Article 12 ISS Act 2002 sets a number of general requirements for data processing including the requirement that the data processing must be necessary for the proper implementation of the ISS Act 2002 or the Security Screening Act. In the case of an administrative check in response to a request for information from a party chairperson, the data processing must be necessary for the performance by GISS of its task, in the interest of national security. In addition, the data must be processed with proper and due care and the data must be accompanied by an indication of reliability or a source reference. Since in the situation under consideration here the data processed are personal data, it must also be examined whether the person in question falls in any of the categories mentioned in Article 13(1) of the Act. Providing the processed data is a separate step, which must be assessed against the statutory requirements set for providing (personal) data to external recipients.

The Committee observes that the policy memorandum makes no mention at all of the fact that the processed data must be accompanied by an indication of the degree of reliability or a reference to the source from which the data have been obtained (Article 12(4) ISS Act 2002).

The policy memorandum does on the other hand devote attention to certain conditions that must have been satisfied before a request for an administrative check can be complied with. The memorandum states that the possibility of calling in GISS does not enter the picture until it emerges, after all means available to the party have been exhausted, that a suspicion exists or continues to exist that a (candidate) political office holder poses a risk in any shape or form to the integrity of the public sector. First of all the Committee observes in regard to this criterion that the integrity of the public sector is not mentioned in the description of the tasks

of GISS as one of the interest which the service is to protect. The Committee points out that the terms "continued existence of the democratic legal order" and "national security or other serious state interests" provide sufficient starting points for investigating certain integrity issues. The Committee considers it important, however, that GISS assesses critically on a case-by-case basis whether the misgivings that have arisen, in combination with the position for which the person in question is eligible, offer sufficient connecting points with the statutory mandate of GISS.

Naturally it is important that GISS is given sufficient information to be able to assess what is the basis for the suspicion of the party chairperson and whether there are sufficient connecting points with the service's statutory mandate. For this purpose the policy memorandum provides that a request for an administrative check must be filed in writing and must state the suspicions that have arisen against (candidate) political office holder and the grounds on which they are based. A policy document on searches and administrative checks by GISS that was recently approved by the service for internal purposes sets an additional requirement for requests from party chairpersons: the request letter must also state the means the party has used itself. This requirement is not included, however, in the policy memorandum furnished to the party chairpersons. The Committee draws the attention of GISS to the fact that if the misgivings that have arisen against a (candidate) political office holder are already sufficiently specific and if the nature of the misgivings shows that it would be useless or even counterproductive for the party to start investigating the matter itself, the mere mention of the misgivings that have arisen may constitute sufficient reason for an administrative check. In other cases the Committee considers it appropriate, for the purposes of assessing the necessity criterion which includes the element of subsidiarity, that the party chairperson states which means the party has used to investigate the misgivings against the (candidate) policy office holder. It recommends that GISS includes a requirement in the policy memorandum that party chairpersons, when filing a request for information with GISS, either state the means which the party has already used to investigate the misgivings, or state brief reasons why the party has not itself used any means.

The group of persons about whom data may be processed pursuant to the policy memorandum consists of the (candidate) political office holders with respect to whom a suspicion exists that they pose a risk to the integrity of the public sector. The Committee holds the opinion that these are persons who fall in one of the following two statutory categories:

1. persons who give cause for serious suspicion that they pose a danger to the democratic legal order, or to national security or other vital state interests (Article 13(1)(a) ISS Act 2002);
2. persons whose data are necessary to support the proper performance by the service of its tasks (Article 13(1)(e) ISS Act 2002).

The Committee holds the opinion that insofar as no cause for serious suspicion exists with respect to the persons regarding whom an administrative check is done, these persons fall in the second category. This is based on the fact that the check is often a necessary first (supporting) step to assess whether there is cause for serious suspicion and for conducting an investigation for the purposes of GISS' task under (a).

The policy memorandum prescribes that GISS must report the findings of the administrative check and/or any investigation conducted pursuant to GISS' task under (a) to the party

chairperson insofar as necessary having regard to the purpose of the administrative check or investigation. This is in accordance with Article 12(2) in conjunction with Article 36 ISS Act 2002. Data must be provided in writing, in accordance with Article 40(1) ISS Act 2002.

With regard to the most recent adjustment of the scope of the policy memorandum[78] the Committee observes that from a legal perspective there are no reasons to exclude regional (candidate) political office holders from these rules in advance. When the nature of the misgivings that have arisen is such that there might be a risk to the interests which GISS must protect given the position to which the person in question is aspiring or which he is holding, it will be lawful for GISS to do an administrative check in its own databases and provide any data found to the party chairperson.

With regard to the restriction of the scope of the rules to candidates for political offices the Committee has asked itself whether it is legally permitted to issue an official message to a party chairperson concerning an incumbent political office holder against whom certain misgivings exist. One objection might be that the party chairperson is not in a position to remove the person in question from office. Viewed in this light the requirement of necessity might preclude issuing such an official message. The Committee finds that it can only be necessary to issue an official message in the interest of national security if the risk posed to national security can be reduced by the measures which the recipient is authorised to take. In the case of incumbent political office holders with respect to whom misgivings exist, the risk to national security lies in the powers attached to the office. For example, the office holder has access to certain rooms, documents and persons and could moreover abuse the attention paid to his or her statements. A party chairperson has a number of means at his disposal to take action against the political office holder. Examples of such measures are that of depriving the office holder in question of his membership of the parliamentary group or of his or her position as spokesperson. It is true that these measures are aimed at changing the position of the office holder within the party, but they will not bring about a reduction of the risk attached to his position as a political office holder. The Committee considers it possible, however, that the party chairperson is in a position to induce the office holder in question to resign by talking to him. Bearing in mind the possible effectiveness of this approach, the Committee therefore holds the opinion that the law does not preclude the issue of an official message concerning an incumbent political office holder.

In view of the special nature of the procedure discussed here, it is the opinion of the Committee that it is important that the policy memorandum provides a clear and complete framework for both party chairpersons and GISS. This requires among other things that the memorandum correctly represents the legal basis pursuant to which GISS may do administrative checks in its own databases. The Committee recommends that GISS adjusts the policy memorandum where necessary.

7.2 Procedure for making official messages to political party chairpersons

The internal procedure for handling a request for information from a party chairperson has been laid down in a policy document drafted in June 2004. This policy document describes the procedure as follows.

[78] The policy memorandum currently relates only to candidate members of parliament instead of the wider concept of (candidate) political office holders.

The first step is that a request from the party chairperson for an administrative check by GISS must be lodged in writing with the minister of the Interior and Kingdom Relations. The request is then passed on to the head of GISS. He examines whether the party itself has used all possible means to investigate the misgivings and assesses whether the seriousness of the suspicion and the gravity of the threatening impairment justify an administrative check and/or (closer) investigation by GISS. The head of the service may be advised on the matter by the legal department and the security officer of the service. If it is decided to comply with the request, the head of the service instructs the security officer to conduct an administrative check in the internal databases. The security officer, acting in consultation with the legal department, reports back the results to the head of the service, adding an opinion whether there is cause to conduct a closer investigation. Subsequently, the security officer, acting in consultation with the legal department, drafts an official message to be issued on behalf of the minister of the Interior and Kingdom Relations to the party chairperson.

The Committee has found in its investigation that in any case since 2007 the internal procedure described in the aforementioned policy documents has not been followed, although it must be noted in this context that since 2007 only one official message was issued as a result of a request for information from a party chairperson. Besides, the Committee was told by GISS that the legal department is no longer involved in issuing official messages to party chairpersons. The Committee therefore recommends that GISS adjusts either its practice or the procedure.

The Committee has not found any evidence that the procedure for making official messages issued to party chairpersons on GISS' own initiative deviates from the usual procedure for making official messages.

7.3 Findings of the Committee

7.3.1 The number of official messages in the review period

In the period from October 2005 – May 2010 GISS issued five official messages to party chairpersons. Three of these messages were issued in reaction to a request for information from the party chairperson. Two messages were issued on the initiative of GISS. All but one of the official messages related to candidate members of the Second Chamber of Parliament. For clarity's sake the Committee notes that the elections to the Second Chamber in June 2010 fell outside the review period and consequently outside the scope of this investigation.

Due to the small number of official messages issued to party chairpersons in the review period, the Committee will discuss some official messages more than once, each time addressing a different aspect of the message.

7.3.2 Legal basis

Since the Designation Order pursuant to Article 39 ISS Act 2002 does not mention political parties or their chairpersons, only Article 36 ISS Act 202 remains as a legal basis for these official messages. This means that official messages to party chairpersons must be issued for the purpose of the performance by GISS of its tasks, in the interest of national security. The Committee holds the opinion that with the exception of one official message, all official

messages issued to party chairpersons in the review period could be based on Article 36 ISS Act 2002.

In 2006 GISS, on its own initiative, issued an official message to a political party concerning a person who had been on the list of candidates for the municipal council, while the service knew that the person in question had not been elected to the council. The Committee makes the following observation. In the case of official messages to party chairpersons, the political office for which the person concerned is a candidate constitutes a link to the interests mentioned in the statutory tasks of the service. This link is absent, however, if the person in question is not or no longer a candidate for political office. In this situation the connection with the tasks of GISS will as a rule be too slight to justify providing information based on Article 36 ISS Act 2002.

The Committee therefore holds the opinion that in this case there was insufficient connection with the statutory tasks of GISS for this official message to be based on Article 36 ISS Act 2002. Consequently, this official message lacks a legal basis and was therefore issued contrary to the closed system of information provision under the ISS Act 2002.

The Committee recommends that GISS makes a record of this fact in the file of the official message (Article 43(2) ISS Act 2002). The Committee does not find it useful in this case to inform the political party in question of the fact that the official message lacks a legal basis.

7.3.3 Content

Three of the five official messages issued by GISS to party chairpersons in the review period provided substantive information. The two other official messages stated that the administrative check had not produced relevant information on the person or persons in question. The Committee has established for two of the official messages providing substantive information that the text of the message was substantiated by the underlying file. These official messages also reflected the underlying information with sufficient care and accuracy.

In the case of the third official message, information was provided orally during a conversation with the secretary of a political party.[79] Prior to this conversation a letter had been sent to the party chairperson stating that GISS had certain information, described in broad terms, concerning an unnamed person who had been on the party's list of candidates for municipal elections. The party chairperson was invited to an interview with the minister of the Interior and Kingdom Relations and the head of GISS. The report of the conversation of the minister and the head of the service with the party secretary does not show exactly what was said about the person in question. It merely states that the party secretary was informed of the name of the municipal council candidate and of the concerns existing with respect to this person. As a result, the Committee cannot trace what exactly was communicated and therefore cannot assess either whether the information provided was covered by the underlying file. Nor can the Committee assess whether the information was formulated with sufficient care and accuracy.

[79] This official message was already discussed above in a different context in section 7.3.2.

7.3.4 Indication of reliability or source reference

In two of the aforementioned three official messages providing substantial information GISS omitted stating the reliability of the information or referring to the source of the information. In one of these messages it was stated that the information "appears from the available data" and the other message (a written confirmation of an oral message) states that GISS had established certain things in the course of performing its regular task.[80]

GISS thus failed to comply with its statutory duty under Article 12(4) ISS Act 2002.

7.3.5 The lawfulness of the underlying data processing

The policy memorandum that is applicable to the procedure for handling a request for information from a party chairperson provides that GISS may only comply with such a request if the party, after using all means at its disposal, finds that a suspicion exists or continues to exists that the (candidate) political office holder poses a risk in any way whatsoever to the integrity of the public sector. This requirement was also included in the older version of the policy memorandum dating from 1998. With this requirement, so the Committee already concluded in section 7.1, the policy memorandum adequately implements the statutory requirements applying to data processing, although the link with the statutory tasks of GISS must be watched carefully.

Three of the five official messages were issued to party chairpersons as a result of a request for information. This means that in those three cases GISS did an administrative check in its own databases. The Committee has found that there was insufficient basis for these checks. In one of these cases the request from the party chairperson was based on an anonymous report received by the candidates committee, to the effect that a candidate for parliamentary elections of this party posed a great risk to the party. In the second case there were signals from various sides about the 'fundamentalist, radical leanings of a candidate in parliamentary elections.[81] In the latter request no misgivings were mentioned at all. The request stated that there were four candidates for parliamentary elections with respect to whom internet searches had not produced sufficiently definite answers.

In the first case, GISS had been provided with too little concrete information to be able to conclude that it was necessary to do an administrative check in its own databases for the purposes of the proper performance by the service of its tasks, in the interest of national security. An anonymous report that a person poses a risk does not constitute sufficient concrete information, since it has not been explained to what the risk relates. In the case of the request for information about four candidates for parliamentary elections where internet searches had not produced sufficiently decisive answers, the party chairperson had likewise provided too little concrete information to constitute grounds on which GISS could base the administrative check.

In the third case: signals from various sides that a candidate in parliamentary elections has fundamentalist, radical leanings, constitute more concrete information. The Committee holds the opinion, however, that it would have been for the party first to question the person concerned and possibly also references and/or informers about the religious ideas of the

[80] This official message was already discussed above in a different context in sections 7.3.2 and 7.3.3.
[81] This official message was already discussed above in a different context in section 7.3.3.

person concerned. Conducting an administrative check without these steps having been taken first, while it was also not clear in advance that questioning the person concerned or persons moving in his circles would be useless or counterproductive, was not in accordance with the statutory criterion that data processing must be necessary for the proper implementation of the ISS Act 2002 or the Security Screening Act, meaning in the case under discussion the proper performance by GISS of its statutory tasks.

7.3.6 Requirements applying to the provision of personal data

Concerning two of the five official messages to party chairpersons the information was provided to the party orally and by text message, respectively.

It was already described in section 7.3.3 how the information was provided in one of these cases. An internal memorandum shows that in this case GISS decided not to provide information in writing because the candidate for municipal elections had not been elected. The Committee points out that if GISS holds the opinion that providing information orally is less infringing than providing it in writing, this opinion is incorrect. Putting down the information in writing makes it possible for the person concerned to defend himself in court at some point in time. It is subsequently always possible to find out which information was provided. Moreover, preparing a written message encourages providing the information more carefully. The legislature has indeed excluded the possibility of providing personal data orally, except in urgent cases. This must always be followed by a written confirmation, stating what personal data have been provided. This did not happen either in the case in question. Due to the absence of a written confirmation and/or a verbatim report of the conversation with the party secretary, it is now no longer possible, as was already observed in section 7.3.3, what was the exact content of what the head of GISS communicated about the candidate for municipal elections in question.

In 2010 the head of GISS informed a party chairperson by text message that no detrimental information had been found in the service's databases concerning the four candidates mentioned in the request.[82] In this case, too, the message was not confirmed in writing as prescribed, in spite of the fact that a report that no detrimental data exist concerning a person definitely constitutes personal data provision.

The Committee holds the opinion that by providing personal data orally and by text message, respectively, without subsequently sending written confirmation of the data provided, GISS acted contrary to Article 40(1) and (2) ISS Act 2002 in both the above cases. This also means that GISS did not comply either with the requirement that records must be kept of any personal data that has been provided (Article 42 ISS Act 2002).

7.3.7 Formal requirements pursuant to the policy memorandum

The irregularities established by the Committee in the preceding sections are also contrary to the rules laid down in the policy memorandum. Furthermore, the policy memorandum sets certain additional procedural requirements which are not laid down by law, but which in the eyes of the Committee promote careful data processing. One of these requirements is that the results of the administrative check must be notified to the party chairperson. The Committee

[82] This official message was already discussed in a different context in section 7.3.5.

has established, however, that in one case GISS first provided the result of an administrative check by telephone to the parliamentary party leader, and in one other case provided information to the party secretary.[83] The Committee points out to GISS that on account of the sensitive nature of the information provision and on account of the employee confidentiality aspects involved, the service should aim at exclusively communicating the results of a administrative check with the party chairperson.

Another requirement of due care that emerges from the policy memorandum is that the request from a party chairperson for an administrative check must be filed with the minister of the Interior and Kingdom Relations in writing. The request filed in 2010 concerning four candidates in parliamentary elections did not satisfy this requirement. In spite of repeated requests to the party chairperson to file a written request with the minister, this took nearly five months. Probably, this had to do with the fact that a mere few weeks after the request GISS had already communicated the results to the party chairperson. Based on the policy, the request should not have been taken up.

For reasons of due care the Committee considers it highly important that the procedure laid down in the policy memorandum is followed, which prescribes that both the request for and the provision of information must be made in writing. It recommends that henceforth GISS will not comply with a request for information until the request has been filed in accordance with the requirements.

7.3.8 Documentation

The Committee has established that it took some time for GISS to produce a list of the official messages that had been issued to party chairpersons in the review period. Furthermore, it emerged from the communications with GISS that it had been difficult for the service to put together the corresponding documents underlying each of the messages, since these documents had not been filed together with the messages.

In the opinion of the Committee the fact that it took some time for GISS to produce a list of the official messages that had been issued to party chairpersons in the review period shows a lack of management in this area. GISS should keep transparent records showing clearly what data has been provided concerning which (candidate) political office holders, especially in view of the sensitivity of this type of information provision. The Committee recommends that GISS keep more transparent records of this category of official messages.

The fact that GISS apparently had not filed the underlying documents together with the official messages shows that it did not adhere to the documentation method prescribed by the 2006 policy document.

The Committee already recommended above in section 7.2 that GISS either formalise in writing the current practice for dealing with a request for information from a party chairperson, or brings its practice in line with the policy document. The Committee finds it important that attention is paid in this context to safeguarding the thorough compilation of complete files. In the case of voluminous files the Committee considers it important that a

[83] These official messages were already discussed in a different context in sections 7.3.5, 7.3.2, 7.3.3 and 7.3.6, respectively.

supplementary memorandum is prepared containing references to the documents underlying the official messages.

8 Official messages to the person charged with forming a new government or the prime minister

8.1 Background and policy

In 2002 the prime minister sent a letter to the Second Chamber informing it about the procedure followed for assessing candidate ministers and vice ministers.[84] The reason for doing so was that there had recently been so many new developments in actual practice that it was considered advisable to reformalize the procedure in writing. After the formation of the government in the summer of 2002, moreover, there had been an incident involving the resignation immediately after her appointment of the vice minister for emancipation, Philomena Bijlhout, because the media had brought to light that she had been a member of the people's militia in Surinam not only before the December Murders in 1982, but still was so at the time they happened.[85] In reply to Parliamentary questions about this incident, the minister of the Interior and Kingdom Relations said he would order an investigation whether it would be advisable to widen the possibilities of screening candidates for government posts.[86] A subsequent letter to the Second Chamber made it clear that there would be no changes to the fact that political offices cannot be designated as offices involving confidentiality. Consequently, it is not possible to subject candidates for government posts to security screening. Their investigation continues to be restricted to an administrative check in the databases of GISS. GISS can only further investigate candidates for a government post if its task under (a) gives cause for doing so.

The procedure laid down in the prime minister's letter of 20 December 2002 and in the manual for government members taking up office[87] is as follows. The person charged with forming a new government holds interviews with each candidate, at which among other things they discuss matters past and present concerning the candidate which form or may form an impediment to his or her taking office. Prior to this interview, three examinations of facts are carried out. By declaring themselves as candidates they are deemed to have given their consent for these examinations. These are an administrative check in the Criminal Records Register, an administrative check for relevant data by GISS in their own databases and an administrative check by the Tax Authorities of the tax file of the person concerned. The result of the check done by GISS is provided to the person charged with forming a new government, who will inform the candidate of any relevant data and discuss them with him or her during the interview. The basic principle is, however, that it is the responsibility of the candidate to raise all relevant facts and circumstances on his or her own initiative.

When a new government member takes up office during the government's term of office, GISS provides the result of the administrative check to the prime minister

---

[84] *Parliamentary Papers II* 2002/03, 28 754, no. 1.
[85] "Resignation vice minister Bijlhout (LPF)" *NRC Handelsblad*, 22 July 2002.
[86] *Parliamentary Papers II* 2001/02, appendix 1465.
[87] *Handboek voor aantredende bewindspersonen,* ministry of General Affairs, dated 25 October 2010, www.rijksoverheid.nl (consulted on 7 April 2011).

The Committee considers the provision of information by GISS about candidates for a government office to be official messages, because the person charged with forming a new government or the prime minister, as the case may be, is authorised to decide as a result of the information that the candidate in question is not eligible for the office. This is not changed by the fact that the information is in principle provided as input for the interview to be held with the candidate. Ultimately, when the information provided by GISS concerns serious facts it can be the decisive factor.

The Committee notes that unlike administrative checks concerning (candidate) political office holders, administrative checks concerning candidates for a government post are not subject to the requirement that there must be a suspicion that the candidate in question in any way poses a risk to national security and/or other serious interests of the state or the democratic legal order. Such a threshold is indeed not necessary in the opinion of the Committee, since it may be assumed that the candidates will have been informed of the administrative check by GISS and have taken this into account in deciding to stand as candidates for a post as minister or vice minister. The situation is therefore comparable to a security screening: the position itself is sufficient cause for doing an administrative check within the scope of the statutory tasks of the service and candidates have agreed (implicitly) to the check being done.

8.2 Procedure for making official messages to the person charged with forming a new government or the prime minister

The applicable policy document of GISS shows that communications about candidates for government posts are not in actual fact conducted with the person charged with forming a new government or the prime minister, but with the secretary-general of the ministry of General Affairs. Request from the secretary-general to GISS to do administrative checks are made orally. The head of GISS notes down the names and dates of birth of the candidates and hands the list to the security officer, asking him to check the databases of the service for relevant data concerning the candidates.

The security officer discusses the result of the administrative checks with the head of the service. If the check regarding a specific candidate has produced relevant data, the security officer prepares a memorandum for the purpose of this discussion, in which he states what information has been found and how the information is characterised. The decision to provide the data to the secretary-general of the ministry of General Affairs is then taken by the head of GISS. This information is provided orally. The policy document prescribes that the head of the service must draw up a report of the conversation with the secretary-general. An interview of the Committee with GISS has shown that in practice the report merely contains a record that the information was provided to the secretary-general on a certain date. Subsequently, a letter confirming with respect to which persons administrative checks have been done is sent to the secretary-general of the ministry of General Affairs. The letter does not, however, include the results of the checks.

The Committee holds the opinion that there are a number of points on which the policy of GISS is not in accordance with the law. Personal data must at all times be provided in writing except in cases of urgency (Article 40(1) and (2) ISS Act 2002). In urgent cases, personal data may be communicated orally, but the communication must be confirmed in writing as soon as possible (Article 40(2) ISS Act 2002). The policy of GISS does not translate

these requirements into specific rules. The head of GISS orally communicates the results of the administrative checks to the secretary-general of the ministry of General Affairs. The Committee has not found any evidence that as a category these cases have such urgency as to make it impossible to prepare an official message – which the head of GISS can, if necessary, hand to the secretary-general in person. In addition, there is no written confirmation of the oral communication. The letter confirming with respect to which persons administrative checks have been done does not suffice in this respect, since it does not state the results of the checks. It is precisely the point of the written confirmation that it shows exactly what was communicated orally.

The Committee therefore recommends that GISS revise the internal procedure and makes it consistent with Article 40(1) and (2) ISS Act 2002. In this context the Committee suggests that GISS involve the legal department in making the messages, just as it is involved in the case of other types of official messages.

8.3 Findings of the Committee

For the purposes of the present investigation the Committee examined 38 files relating to the administrative checks done for the purposes of the parliamentary elections in 2007 and the subsequent government formation. In addition to these, three administrative checks were done in connection with persons taking up government posts in between elections. The administrative checks done for the purposes of the government formation in 2010 fall outside the scope of this investigation.

The Committee has found that two of the 38 administrative checks done by GISS in 2007 with respect to candidates for government posts produced data that was relevant in the context of the tasks of GISS. The three checks done in between elections did not produce any relevant data. The written confirmations of the administrative checks in 2007 sent to the secretary-general of the ministry of General Affairs in accordance with policy, mention one case in which information was provided. Since there is no record whatsoever of this information provision, it proved impossible for the Committee to find out in which of the two likely cases information was actually provided to the secretary-general of the ministry of General Affairs. Nor is it now possible to establish the content of the information. As a result, the Committee is unable to assess whether the content of this official message satisfied the statutory requirements.

As was already observed in the preceding subsection, GISS' policy does not implement the statutory requirement that personal data must be provided in writing unless there are reasons for urgency. It is true that the applicable policy document provides that the head of the service must draw up a report of his conversation with the secretary-general. If this report should state exactly what data relating to candidates for government posts has been provided to the secretary-general, this would in the opinion of the Committee satisfy the requirement that a record must be kept of any provision of personal data (Article 42 ISS Act 2002). The Committee's investigation has shown that in recent practice the report merely contains a record that the information found was provided to the secretary-general on a certain date. As regards the provisions of information in 2007, either no record was made at all of reporting back to the secretary-general, or these records have not been filed in a retrievable way.

In the opinion of the Committee both the policy and its implementation by GISS in 2007 fall seriously short of what is required. It is noticeable that the entire procedure has an informal structure. Names and dates of birth of the candidates are stated orally to the head of GISS, he notes them down and instructs the security officer to do the administrative checks. The results of the checks are also reported back orally, without subsequent written confirmation of what personal data has been provided. As observed above, the written confirmation administrative checks does not suffice, because it does not include the result of the administrative checks. At best, the head of GISS records that he has reported back the results of the administrative checks to the secretary-general. In any case he does not record what exactly he told the secretary-general.

The Committee suspects that the political sensitivity of the provision of information concerning candidates for government posts played a role in the fact that GISS has opted for a procedure in which it does not lay down very much in writing. The Committee emphasizes, however, that the sensitivity of such provisions of information is precisely a reason for thoroughly recording all the steps in writing.

9 Official messages to other recipients

9.1 Types of official messages to other recipients

In addition to the recipients of official messages discussed in the preceding sections, GISS also issues official messages to other bodies. The most frequent categories are mentioned below.

GISS contributes to the enforcement of the freezing lists of the EU and the UN by stating whether a specific person is identical with a person included in one of these lists.[88] If the financial institutions have insufficient certainty that a person on one of the lists is identical with a person included in their files, this is known as a "possible hit". At this stage the institutions do not freeze the bank balances of the person in question yet. In such a case GISS is requested to start investigating the possible hit. This investigation is restricted to an administrative check in GISS' own databases and, if necessary, the collection of relevant data using its general powers under Article 17 Act 2002. If GISS succeeds in establishing that it is an "exact hit" or if there are special circumstances, GISS will inform the ministry of Finance and if appropriate the National Public Prosecutor of this fact by means of an official message. Since 2005 an arrangement has been in place that GISS will not issue an official message if GISS is unable to give an opinion on the matter.

Another role of GISS in the context of the freezing lists is that of proposing persons and organisations for freezing measures. For this purpose an official message is issued to the ministry of Foreign Affairs. Based on such an official message the ministry of Foreign Affairs may convene an interdepartmental consultative freezing meeting, which in addition to GISS

[88] See for a more detailed consideration of this issue the Committee's review report no. 20 on financial and economic investigations by GISS, *Parliamentary Papers II* 2008/09, 29 924, no. 35 (annex), see also www.ctivd.nl.

is attended by the ministry of Finance and the National Coordinator for Counterterrorism and Security. Pursuant to Article 40 ISS Act 2002, GISS may grant inspection of the documents underlying the official message to the authorities involved in the freezing consultations. If the consultations result in a freezing measure, the minister of Foreign Affairs issues a sanctions measure. Subsequently, it may be decided whether the Netherlands will attempt to propose the person or organisation in question at the EU or the UN as a sanction target.

Furthermore, GISS may issue a message to the ministry of Foreign Affairs stating whether there is cause to maintain a freezing measure. Such official messages are issued in response to a request for information from the ministry of Foreign Affairs for the purpose of the regular review of freezing measures. At the interministerial level it has been agreed to review national sanctions measures every six months. EU or VN freezing measures can only be terminated in accordance with the applicable international procedures. Member states can request the removal of a person or organisation from the UN or EU freezing list. At the interministerial consultative meetings the persons and organisations that have been included in an international freezing list at the proposal of the Netherlands are examined every six months. When GISS has not responded to a request for information from the ministry of Foreign Affairs within 15 working days, this means that the service sees no cause to maintain the freezing measure in question, or that there are no reasons that can be disclosed for maintaining the freezing measure.

In addition to providing information for the purpose of freezing measures, GISS occasionally provides information to the ministry of Foreign Affairs in connection with visa applications. The ministry of Foreign Affairs deals with visa applications for the purposes of *inter alia* business visits, diplomatic affairs, conferences and visits of a political nature. The same 'silent procedure' that applies to the regular reviews of freezing measures, applies to requests to GISS for information from the ministry of Foreign Affairs: GISS will issue an official message when it has found that there is cause to do so in the interest of national security.[89]

When in the course of performing its tasks GISS obtains information that is relevant to maintaining public order, this information may be provided to the relevant mayor by means of an official message. Usually, official messages to mayors relate to demonstrations planned by extremist groups or to organisations receiving municipal subsidies. Official messages for the purpose of maintaining public order may also be issued to regional chiefs of the police force.

Finally, GISS sporadically issues official messages to other persons and bodies. It may, for example, inform an employer of security-relevant information with respect to an employee or alert the customs to security-relevant information concerning travellers.

9.2 Procedure for making official messages to other recipients

A detailed discussion of the particulars of the specific procedures for making the different types of official messages described in the preceding subsection would go beyond the scope

[89] See also the Committee's review report no. 13 on the exchange of information between GISS and the Immigration and Naturalisation Service, *Parliamentary Papers II* 2006/07, 29 924, no. 19 (annex), section 5.1.4, See also www.ctivd.nl.

of the present investigation. In all cases the general structure of these procedures is that first the text of the message is drafted by the team concerned, then the text and the underlying file are coordinated with the legal department and subsequently the message and the file are approved by the team head, the legal department, the unit head and the service management.

9.3 Findings of the Committee

9.3.1 The number of official messages issued in the review period

In the review period a total of 42 official messages were issued to recipients in the category of other recipients, of which 23 were issued to mayors and chiefs of police, and the rest to the ministry of Finance, the ministry of Foreign Affairs, the chief of the National Police Force, the customs, Interpol, the Royal Netherlands Military Constabulary and a place of detention. The Committee noticed that the ministry of Finance did not receive any official messages in the final years of the review period. This may be due to a revised procedure for implementing freezing measures, according to which GISS is only required to issue an official message if information is available.[90]

9.3.2 Legal basis

As a rule, official messages to recipients other than the Public Prosecution Service must be issued under Article 36 ISS Act 2002 and therefore for the purpose of the performance by GISS of its tasks, in the interest of national security. An exception to this rule is the provision of information for an urgent and serious reason pursuant to Article 39 ISS Act 2002. The Designation Order under Article 39 ISS Act 2002 shows that under Article 39 data may be provided to ministers, mayors, the Dutch central bank Nederlandsche Bank N.V. and the financial markets authority Stichting Autoriteit Financiële Markten.

The Committee has established that the official messages which GISS issued to other recipients in the review period were rightly based on Article 36 or Article 39 ISS Act 2002.

9.3.3 Content

The official messages issued to other recipients investigated by the Committee are substantiated by the underlying information. The wording of a number of official messages calls for some observations, however.

In 2006 GISS issued two official messages to the ministry of Foreign Affairs for the purpose of freezing measures against the financial assets of two persons. The Committee made several remarks about these official messages in the secret annex to its review report on financial and economic investigations by GISS. In the present review report it will suffice to

[90] Review report of the Committee no. 20 on financial and economic investigations by GISS, *Parliamentary Papers II* 2008/09, 29 924, no. 35 (annex), section 5.7.3, see also www.ctivd.nl.

note that there is one term that is used in the official messages which in the opinion of the Committee is not sufficiently clear and concrete.

The Committee has further established that in the review period GISS issued two official messages to mayors relating to demonstrations. The messages stated that the protesters intended using everyday items that can be used as (striking) weapons. The Committee has found that in these cases GISS used this description to refer to a variety of items. It is open to question whether it was clear to the recipient what it should understand this term to mean. In this case, too, GISS should in the opinion of the Committee have chosen a more concrete wording.

9.3.4 Indication of reliability or source reference

The Committee's investigation has shown that the official messages in the category under discussion usually contain an indication of reliability or a source reference.

An exception is an official message issued in 2009 to the ministry of Foreign Affairs in connection with a visa application. In this message GISS recommended that the ministry should refuse a visa application for reasons of national security. No further explanation of these reasons was given. Moreover, the message did not state whether the information was reliable. The Committee holds the opinion that this means that GISS has not complied with its statutory obligation under Article 12(4) ISS Act 2002.

In 2010 GISS issued an official message containing a report that a certain group was planning an action. The information, qualified as reliable, originated mainly from a human source. However, the Committee has not found a reliability memorandum regarding this human source in the file. This is not in keeping with the policy at GISS. Due to the absence of an assessment of the reliability of the information it is impossible to verify on the basis of the underlying file whether the indication of reliability in the message is correct.

9.3.5 Documentation

The Committee has established that the files of the official messages in the category under consideration were usually complete and transparent. There is one file on which the Committee wishes to make a comment.

In 2009 GISS informed the customs of certain information relating to the luggage of a passenger. This enabled the customs to search the luggage. It is true that certain indications emerged from the file examined by the Committee, but these were insufficient to substantiate the official message. GISS told the Committee that the official message was actually based on information from a human source. At the time of issuing the official message this had not yet been laid down in writing in an intelligence report. Subsequently, the intelligence report was drawn up, but not added to the documents underlying the official message. The supplementary memorandum to the official message does not mention this information either. The Committee considers this procedure to be negligent, since the official message was based predominantly on the information from the human source.

10 Conclusions and recommendations

Official messages issued to the Public Prosecution Service

10.1 In the opinion of the Committee all but one of the official messages issued by GISS to the Public Prosecution Service are rightly based on Article 38 ISS Act 2002. The Committee holds the opinion that in one case GISS wrongly opted to provide data to the Public Prosecution Service. There were no indications that the person concerned had committed any offences. Given the office held by the person concerned, GISS could in this case have opted to issue an official message to his employer pursuant to Article 36 ISS Act 2002. (section 4.4.2)

10.2 In the course of its investigation the Committee came across two cases in which GISS provided data to the Public Prosecution Service which GISS knew to be already in the possession of the Public Prosecution Service. In both cases the Committee found that by issuing the messages GISS sought to influence the follow-up steps to be taken by the Public Prosecution Service.
However, issuing an official message containing information that is already known to the recipient is not the appropriate procedure for achieving this. When GISS has specific wishes or advice concerning the steps which the Public Prosecution Service should undertake in a certain investigation, it can consult with the Service – through the National Public Prosecutor. The Committee holds the opinion that in such cases the provision of information is not necessary for the purpose of the investigation and prosecution of offences since the Public Prosecution Service already has the information. (section 4.4.3)

10.3 The Committee has found that the content of the official messages issued by GISS to the Public Prosecution Service in the review period is substantiated by the underlying files. In a number of cases, however, GISS should have exercised greater care in formulating the message. (section 4.4.4)

10.4 The policy of GISS regarding the provision of detailed information to the Public Prosecution Service is that there must be urgent reasons to provide such information in the context of the tasks of GISS. The Committee holds the opinion that in this respect GISS exercises greater restraint than was envisaged by the legislature. It points out that the interests of investigation and prosecution must carry great weight. Whenever it is possible for GISS to reveal (detailed) information, it should only decide not to do so if providing the information would harm the interests of the service. (section 4.4.5)

10.5 The Committee has established that as a rule GISS consistently includes an indication of reliability in the official messages to the Public Prosecution Service. Two related official messages issued in 2006 and an official message issued in 2008 are an exception to this rule. (section 4.4.6)

10.6 In its investigation the Committee came across some examples of official messages to the Public Prosecution Service in which information from one single human source formed the basis of part of the message. The Committee holds the opinion that in these cases GISS exercised due care in establishing the reliability of the information. (section 4.4.6)

10.7 The Committee points out that because GISS does not include exculpatory information which it has not found reliable in the file underlying official messages, such information will not be found by the National Public Prosecutor who checks the content of the official messages issued to the Public Prosecution Service. It will also not be possible for the Committee to review the assessment in retrospect. As a result, the assessments made by GISS regarding the reliability of this information are unverifiable. In the opinion of the Committee it is advisable to arrange the files underlying official messages in such a way that they show whether exculpatory information is available and how GISS assessed the reliability of this information. (section 4.4.7)

10.8 In connection with two official messages to the Public Prosecution Service the Committee saw reason to investigate the underlying use of special powers. In both cases the special powers were used in an intelligence investigation conducted in parallel with a criminal investigation. The Committee holds the opinion that in view of the relevant facts and circumstances the powers were used lawfully in these two cases. (section 4.4.8)

10.9 The Committee has established that generally the official messages that have been issued to the Public Prosecution Service are supported by thorough documentation. In one case GISS added an earlier official message on the relevant persons to the file of a subsequent official message to substantiate certain information. It is the opinion of the Committee that in such cases GISS should add (copies of) the relevant documents from the file of the earlier official message to the new file. (section 4.4.9)

Official messages issued to the Immigration and Naturalisation Services (INS)

10.10 The Committee recommends that GISS correctly sets out in the applicable policy document the legal basis for doing an administrative check at the request of INS as well as the related statutory requirements. (section 5.2)

10.11 The Committee has found that in practice the requests from INS always lead to an administrative check by the front office of GISS, which is where these requests are received. The front office conducts the check to examine whether the request can be passed on to a specific team, which will then further deal with the request. Since this first check is a form of data processing, the Committee holds that GISS must first assess the request against the requirement of necessity before it tries to link it to a team. The assessment can be made using the form supplied by INS which among other things states the reason for the request for information. (section 5.2)

10.12 The Committee recommends that GISS, in consultation with INS, formalises the current practice of exchanging information between GISS and INS in a written procedure as soon as possible. (section 5.2)

10.13 The legal basis for providing data to INS for the purpose of the performance by GISS of its tasks, in the interest of national security, is Article 36 ISS Act 2002. The Committee holds the opinion that the official messages issued by GISS to INS in the review period could be based on Article 36 ISS Act. (section 5.3.2)

10.14 The Committee's investigation has shown that all but one of the official messages issued by GISS to INS in the review period are substantiated by the underlying

information. The messages are, moreover, carefully formulated, so that they are in line with the underlying information. (section 5.3.3)

10.15 The Committee has found that GISS does not use a consistent definition of the term "threat to national security". GISS considers on a case-by-case basis whether this conclusion applies. Each of the official messages examined by the Committee concerned activities having such a clear connection with national security, that in the opinion of the Committee they justified the conclusion. (section 5.3.3)

10.16 The Committee draws the attention of GISS to the fact that it is important for the alien about whom the service issues an official message that he receives sufficient factual information at the earliest possible stage. When the protection of sources, the secrecy of the current level of knowledge and/or the operational methods of the service or the third party rule do not constitute a reason to withhold concrete details, then in the opinion of the Committee GISS should therefore seek to provide INS with as much concrete information as possible. (section 5.3.3)

10.17 The Committee has established that the official messages issued by GISS to INS contain an indication of reliability. In one case the Committee has established that with respect to part of the information provided the indication of reliability in the official message was not substantiated by the underlying file. In this respect the official message is unlawful. The Committee therefore recommends that GISS records this in the relevant file pursuant to Article 43(2) ISS Act 2002 and informs INS that the reliability of the sources on which the first part of the official message is based has not been established. (section 5.3.4)

10.18 The Committee has found that when the Regional Intelligence Services provide information to GISS pursuant to Article 60 ISS Act 2002, they often omit including an indication of the reliability of the information. Where they have included a reliability indication, the indication is often ambiguous, since different coding systems and qualifications are used. This way of processing information is contrary to Article 12(4) ISS Act 2002. The Committee recommends introducing clear and unambiguous indications of the reliability of the information which the Regional Intelligence Services pass on to GISS. (section 5.3.4)

Official messages issued to the ministry of Economic Affairs, Agriculture and Innovation (EAA&I)

10.19 The Committee has found that GISS has started consultations with the ministry of EAA&I about laying down the arrangements in the field of information provision in a covenant. The Committee endorses the usefulness of such a covenant. (section 6.1)

10.20 Taking into consideration that the information provided to the ministry of EAA&I in connection with export applications will by definition reveal the current level of knowledge of GISS regarding companies in countries of concern, the Committee holds the opinion that the classification of these official messages is justified. It holds the opinion that in those cases the general interest of national security must carry greater weight than the individual interest of the exporter in learning the content of the official message. (section 6.3.2)

10.21 The Committee recommends that GISS, in consultation with the ministry of EAA&I, seeks ways to promote that the ministry can make its decisions on the basis of an

adequate information position. One possibility is that of granting the ministry of EAA&I, where necessary, inspection of the documents underlying the official messages. (section 6.3.2)

10.22 The Committee expects that the use of a matrix of standard phrases will promote consistency in the official messages issued to the ministry of EAA&I. The formalisation of the different standard phrases has produced clarity. The Committee considers it important, however, that GISS assesses for each official message separately whether the chosen standard phrase adequately represents the underlying information and whether it is possible to provide more factual information than the standard phrase without affecting the agreements made with foreign counterpart services and the secrecy of sources, current level of knowledge and/or operating procedure of the service. (section 6.3.3.1)

10.23 It has emerged from the Committee's investigation that GISS, which formerly did not consider the messages to the ministry of EAA&I to be official messages, did not always set very high requirements on the substantiation of the messages. It is the opinion of the Committee that in two cases the official message is not substantiated by the underlying information. These official messages were not made with proper and due care and are therefore unlawful. The Committee recommends that GISS, pursuant to Article 43(2) ISS Act 2002, makes a record of this fact in the relevant file and informs the ministry of EAA&I, with a view to possible future applications for export licences for the benefit of the end-users concerned, that the two aforementioned official messages are not substantiated by the information in the possession of the service. (section 6.3.3.2)

10.24 The Committee has found that the official messages issued by GISS to the ministry of EAA&I in the early part of the review period usually do not contain an indication of reliability. This means that in this period GISS did not comply with the statutory requirement of Article 12(4) ISS Act 2002. From early in 2009 GISS has included an indication of reliability in the official messages. (section 6.3.5)

10.25 Information from human sources is seldom used in official messages to the ministry of EAA&I. The Committee has established that the Counter Proliferation Unit, unlike the other departments of GISS, does not prepare reliability memorandums for the underlying file in such cases. This is not in keeping with general policy at GISS in this area. The Committee recommends that the Counter Proliferation Unit adjusts its procedure. (section 6.3.5)

10.26 The Committee holds the opinion that the data provided by GISS to the ministry of EAA&I is not personal data. Nevertheless, the Committee finds that where data is provided which may result in measures being taken against persons or companies, the same proper and due care must be exercised as in the case of the provision of personal data. Because of the potential consequences of the provision of such data the Committee considers it appropriate that the special requirements of proper and due care mentioned in Articles 40, 41 and 42 IIS Act 2002 apply to the official messages to the ministry of EAA&I. (section 6.3.6)

10.27 The Committee holds the opinion that the policy of the Counter Proliferation Unit satisfies the requirements of due care to a sufficient degree. The Committee has found that the Counter Proliferation Unit observes the policy, with a few exceptions. In one

case information was provided which dated back twelve years. The Committee points out that if this information was deemed so incriminating that it could not be disregarded, the official message should in any case have mentioned the degree of reliability and the age of this information, which did not happen in this case. The Committee considers this to be negligent. The Committee has established that in two cases oral information was communicated from the Counter Proliferation Unit to the ministry of EAA&K that 'something' had been found. The exact content of these communications can no longer be retrieved. The Committee holds the opinion that for reasons of due care the service must refrain from making such remarks in its contacts with the ministry of EAA&I. (section 6.3.6)

10.28 Sometimes, only the relevant pages of large documents are included in the files of the official messages issued to the ministry of EAA&I, or it is otherwise impossible to retrieve from which document the pages are taken. The Committee recommends that in such cases the Counter Proliferation Unit indicates what is the document concerned and mentions its date. (section 6.3.7)

Official messages issued to political party chairpersons

10.29 When a party chairperson has addressed a request to GISS for information concerning a (candidate) political office holder, the Committee considers it appropriate, for the purposes of assessing the necessity which includes the element of subsidiarity, that the party chairperson states which means the party has already used to investigate the misgivings against the (candidate) policy office holder. The Committee recommends that GISS include a requirement in the policy memorandum applicable to this procedure and furnished to the party chairpersons, that party chairpersons either state the means which the party has already used to investigate the misgivings, or state reasons why the party has not itself used any means. (section 7.1)

10.30 In view of the special nature of the procedure for providing information to party chairpersons, it is the opinion of the Committee that it is important that the applicable policy memorandum provides a clear and complete framework for both the party chairpersons, to whom the memorandum is furnished, and GISS. This requires among other things that the memorandum correctly sets out the legal basis pursuant to which GISS may do administrative checks in its own databases. The Committee recommends that GISS adjusts the policy memorandum where necessary. (section 7.1)

10.31 The Committee has found in its investigation that the internal procedure followed in practice for dealing with a request for information from a party chairperson differs from the procedure described in the applicable policy document. The Committee therefore recommends that GISS adjusts either its practice or the procedure. (section 7.2)

10.32 The legal basis for providing information to the political party chairpersons is Article 36 ISS Act 202. This means that these official messages must be issued for the purpose of the performance by GISS of its tasks, in the interest of national security. The Committee holds the opinion that with the exception of one official message, all official messages issued to party chairpersons in the review period could be based on Article 36 ISS Act 2002. The Committee holds the opinion that in one case there was

insufficient connection with the statutory tasks of GISS for this official message to be based on Article 36 ISS Act 2002. Consequently, this official message lacked a legal basis and was therefore issued contrary to the closed system of information provision under the ISS Act 2002. The Committee recommends that GISS makes a record of this fact in the file of the official message (Article 43(2) ISS Act 2002). It does not find it useful in this case to inform the political party in question of the fact that the official message lacked a legal basis. (section 7.3.2)

10.33 Three of the five official messages issued by GISS to party chairpersons in the review period provided substantive information. In two cases the Committee has been able to establish that the text of the message was substantiated by the underlying file. These messages also represented the underlying information with sufficient care and accuracy. In the third case, information was provided orally. The report of the conversation does not show exactly what was said about the person in question. As a result, the Committee cannot trace what exactly was communicated and therefore cannot assess either whether the information provided was covered by the underlying file. Nor can it be assessed whether the information was formulated with sufficient care and accuracy. (section 7.3.3)

10.34 In two of the three official messages providing substantial information to party chairpersons GISS omitted stating the reliability of the information or referring to the source of the information. GISS thus failed to comply with its statutory obligation under Article 12(4) ISS Act 2002. (section 7.3.4)

10.35 The Committee has found that the basis for the administrative checks done in response to requests for information from a party chairperson was insufficient in three of these cases. In two cases GISS had been provided with too little concrete information to be able to conclude that it was necessary to do an administrative check in its own databases for the purposes of the proper performance by the service of its tasks, in the interest of national security. In one case the Committee holds the opinion that it would have been for the party to first investigate the misgivings that had arisen itself. (section 7.3.5)

10.36 The Committee holds the opinion that in two cases in which GISS provided personal data orally and by text message, respectively, without subsequently sending written confirmation of the data provided, GISS thus acted contrary to Article 40(1) and (2) ISS Act 2002. This also means that GISS did not comply either with the requirement that records must be kept of any personal data that have been provided (Article 42 ISS Act 2002). (section 7.3.6)

10.37 For reasons of due care the Committee considers it highly important that the procedure laid down in the policy memorandum is followed, which prescribes that both the request for and the provision of information must be made in writing. It recommends that henceforth GISS will not comply with a request for information until the request has been filed in accordance with the requirements. (section 7.3.7)

10.38 In the opinion of the Committee the fact that it took some time to produce a list of the official messages that had been issued to party chairpersons in the review period shows a lack of management in this area. GISS should keep transparent records showing clearly what data has been provided concerning which (candidate) political office holders, especially in view of the sensitivity of this type of information

provision. The Committee recommends that GISS keep more transparent records of this category of official messages. (section 7.3.8)

Official messages to the person charged with forming a government or the prime minister

10.39 The Committee holds the opinion that the internal procedure for making official messages to the person charged with forming a government or the prime minister is not in accordance with the statutory requirements applying to the external provision of personal data. The Committee therefore recommends that GISS revise the internal procedure and make it consistent with Article 40(1) and (2) ISS Act 2002. In this context the Committee suggests that GISS involve the legal department in making the messages, just as it is involved in the case of other types of official messages. (section 8.2)

10.40 The Committee has found that two of the 38 administrative checks done by GISS in 2007 with respect to candidates for government posts produced data that was relevant in the context of the tasks of GISS. The written confirmation of the administrative checks sent to the secretary-general of the ministry of General Affairs, however, mentions one case of information provision. Since there is no record whatsoever of this information provision, it proved impossible for the Committee to find out in which of the two likely cases information was actually provided to the secretary-general of the ministry of General Affairs. It is also no longer possible to establish the content of the information. As a result, the Committee is unable to assess whether the content of this official message satisfied the statutory requirements. (section 8.3)

Official messages to other recipients

10.41 The Committee has established that the official messages which GISS issued to other recipients in the review period were rightly based on Article 36 or Article 39 ISS Act 2002. (section 9.3.2)

10.42 The official messages issued to other recipients investigated by the Committee are substantiated by the underlying information. The Committee holds the opinion that in three cases GISS should have chosen more clear and concrete wordings. (section 9.3.3)

10.43 The Committee's investigation has shown that the official messages issued to other recipients in the review period usually contain an indication of reliability or a source reference. One exception is an official message issued in 2009 to the ministry of Foreign Affairs. (section 9.3.4)

10.44 The Committee has established that the files of the official messages in this category were usually complete and transparent. With respect to one file the Committee observes that the information constituting the main basis of the message had not been included in the underlying file nor in the supplementary memorandum. The Committee considers this to be negligent. (section 9.3.5)

Thus adopted at the meeting of the Committee held on 28 September 2011.