COMMISSIE VAN TOEZICHT
BETREFFENDE
DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

summary and conclusions
of the

REVIEW REPORT

on

the classification
of state secrets
by GISS

CTIVD no. 33

13 June 2012

REVIEW COMMITTEE
FOR THE
INTELLIGENCE AND SECURITY SERVICES

CTIVD no. 33

SUMMARY

Of the review report on the classification of state secrets by GISS

In performing its task the General Intelligence and Security Service (GISS) handles information which is to a considerable extent state secret information. State secret information concerns the interests of the State or its allies. It is imperative to prevent state secret information from coming to the knowledge of unauthorized persons. State secret information must be designated as state secret in the prescribed manner. Designating information as state secret is known as classification. The Review Committee for the Intelligence and Security Services (further referred to as: the Committee) has investigated whether GISS applies the classification of state secrets correctly.

When classifying information GISS must work within the applicable legal framework. The Committee refers in particular to the provisions of the Civil Service Information Security (Classified Information) Regulations (further referred to as: the "Classified Information Security Regulations"). It is important to recognize that information should only be classified as state secret if it is necessary in the interest of the State or its allies. This principle implies that GISS should aim at classifying as little information as possible. The Committee emphasizes that the principle is not only based on cost-saving reasons, but may also have the effect of promoting transparency.

The Committee has established in the course of its investigation that GISS has hardly elaborated the general rules embodied in the Classified Information Security Regulations in its internal rules. The internal rules are outdated, not widely available within the organisation or fail to provide a sufficient basis to go upon in actual practice. The Committee considers it important that GISS lays down a more detailed, practice-oriented elaboration of the classification guidelines. It points out that the Classified Information Security Regulations require such elaboration as well. The Committee thinks it important that GISS, when adopting detailed rules, gives particular attention to the criteria for the different classification levels.

In spite of the absence of an internal detailed legal framework the Committee has come to the conclusion that the classification process generally proceeds correctly. This holds particularly true for the classification of operational information, i.e. information directly relating to the performance by GISS of its task. In the Committee's opinion the state secret classification by GISS of information relating only indirectly to the performance of its task is more debatable, in particular in the field of personnel policy at GISS.

The Committee has established that in particular the dividing line between state secret - CONFIDENTIAL and state secret - SECRET can be said to be rather fluid and to a certain extent subjective. In particular with respect to internal products the use of either the one or the other classification level has hardly any practical consequences.

In view of this situation the Committee considers advisable that GISS aims at greater internal awareness of the classification process. A detailed, practice-oriented internal framework can have added value in achieving this. The Committee has also seen reason to recommend that the structural internal supervision at GISS of classification practice will be enshrined more firmly in the organisation.

In regard to the external provision of state secret information, i.e. state secret information provided to end-users outside GISS, the Committee observes that it has found that it is not always clear to end-users what is the state secret element in the information. If GISS would, as far as possible, indicate for each paragraph whether or not it is state secret, this will also lead to greater recognition of the added value by the end-user. At the same time it will prevent erosion of the security regulations, because there is a risk that the security regulations will be applied less strictly if it is not clear why information must be kept secret.

The Committee has established that GISS usually does not state on classified documents what is the classification expiry date. The Classified Information Security Regulations provide for a maximum classification period which varies from ten to twenty years, depending on the type of information. The Committee points out that this is a *maximum* classification period and that a shorter classification period should be applied whenever possible. The Committee considers advisable that GISS states for each document what is the expiry date of the classification. Expiry dates can be based on classification guidelines to be set out in detail.

In this context the Committee has further established that GISS lacks a structural declassification programme. GISS does not examine the possibility of adjusting or terminating the classification of information after some time. The Committee points out that the Classified Information Security Regulations do in fact impose this active obligation on GISS and that GISS has also included the relevant provision in its own internal rules. In practice, the classification of information is only revised in the context of issuing an official message or dealing with applications for inspection of information processed by or on behalf of the services (known as applications for inspection of files).

The Committee has furthermore established that the service has still not adopted a selection list based on which it can proceed to transfer records to the National Archives or destroy data that are no longer relevant. The ongoing discussion on the subject which has been at a deadlock for years will have to be decided. The Committee considers advisable to adopt a partial selection list with regard to points on which there is no division of opinions. Because there is no selection list, GISS must keep all data in a durable form. This applies to both digital data carriers and paper records. Eventually, this will obviously lead to considerable storage costs. The Committee thinks it likely that the high storage costs will, at any rate in the future, exceed the costs of an active declassification programme, for example in the form of additional manpower.

The Committee is aware that it is difficult to find the right balance between secrecy and transparency. It is not easy for an intelligence and security service to operate inherently and necessarily with a high degree of secrecy, while at the same time providing the transparency required to maintain the trust of society. The Committee perceives an increasing demand in society for greater transparency, also from the intelligence and security services. In addition, with increasing frequency and intrusiveness information provided by GISS to external end-users is subjected to review by the courts for transparency.

13 Conclusions and recommendations

THEORY

13.1 GISS must protect its sources, particularly with a view to their safety. It is the opinion of the Committee that the duty to ensure the secrecy of sources applies exclusively in respect of *human* sources of GISS. A technical source, such as a telephone tap, is not a source within the meaning of article 8(3)(b) ISS Act 2002. (section 3.4.1)

13.2 It is the opinion of the Committee that state secret nature of the methods used by GISS is not permanent and that a connection can be seen to exist with the protection of its current level of knowledge. In the Committee's opinion the use of a special power by GISS is only state secret in nature if the information about the use is relevant to an ongoing investigation of GISS or if it reveals the level of technical knowledge of GISS. If the fact that a special power has been used with respect to a target no longer has any relevance whatsoever to any ongoing investigation, this puts an end to its state secret nature. (section 3.4.2)

13.3 Information should only be classified as state secret if the information in question relates to an ongoing investigation of GISS or if it is relevant to another ongoing investigation of GISS. The Committee holds that if this is not the case, there is no necessity to classify the information as state secret. (section 3.4.3)

13.4 Personal data that are relevant to any ongoing investigation must be classified as state secret to protect the current level of knowledge. Although the law does not contain a similar provision relating to administrative matters, the Committee holds the opinion that the same rule applies to information other than personal data. (section 3.5)

PRACTICE

Internal policy and practice at GISS

13.5 The Committee has established that some GISS staff members assume that the need to classify information and the application of the *need to know* requirement serve the same purpose, in the sense that they will use a higher classification level to ensure that the information does not come to the knowledge of too many persons *within* GISS. The Committee holds the opinion that classification is not the appropriate means for achieving the latter. Instead, GISS should work with authorized access groups to maintain the *need to know* principle (compartmentalisation). **It recommends that GISS brings this principle clearly into the limelight within the organisation and ensures that no unnecessarily high classification level is assigned to information for the above reason if the nature of the information itself does not require the higher classification level.** (section 6.1)

13.6 The Committee has established that in practice GISS, when classifying information, does not state the expiry date of the classification. The Committee considers this procedure to be contrary to the provisions of the Classified Information Security Regulations. **It recommends that when GISS classifies information it states at the**

same time, in conformity with article 5(4) of the Classified Information Security Regulations, when the classification can in principle be terminated. (section 6.1)

13.7 **The Committee recommends that GISS updates the classification list in such a way as to give it practical added value. GISS should moreover ensure that the classification list is widely available within the service and is actively brought to the attention of its employees.** The Committee believes that the security officer can play a role here. The Committee also draws attention to the task of the secretary-general of the ministry of the Interior and Kingdom relations, who is charged pursuant to article 13 of the Classified Information Security Regulations with supervising correct compliance with the Classified Information Security Regulations. (section 6.1)

13.8 The Committee has established that the issue of guidelines for classifying specific types of information, for example certain operational plans or tapping records, is addressed in internal documents on an occasional basis. It is the opinion of the Committee that at GISS such guidelines have not been documented in a sufficiently accessible manner. (section 6.1)

13.9 The Committee has established that a need is felt at GISS at staff level for a more detailed specification of the classification rules. **The Committee recommends that GISS, paying regard to the foregoing including the basic principles derived from case law, provides an elaboration of the Classified Information Security Regulations tailored to practical needs, which as far as possible provides concrete handles for the classification of documents produced by GISS. These detailed rules should pay particular attention to the different classification levels and the criteria applying to each of them.** (section 6.1)

13.10 The Committee observes that GISS has established that certain end-users will take a higher classification level more seriously and that it is therefore worthwhile to use higher classification levels. The Committee can understand this operational principle, but holds the opinion that it is not in conformity with the Classified Information Security Regulations. (section 6.2)

13.11 **The Committee considers it proper for GISS to enshrine the central supervision of consistent application of the classification rules more firmly in the organisation than is presently the case.** (section 6.2)

13.12 The Committee holds that it is not conducive to consistent classification throughout the service that the considerations for classifying a document are but poorly set out in the written opinions of the Supervisory Department. **It recommends adjusting the procedure to make it possible to meet the Classified Information Security Regulations' objective of examining information after some time to see whether it may be declassified and to facilitate decision-making on this point.** (section 6.2)

Classification of operational information

13.13 The Committee has established that by far the most part of the information laid down by GISS does in some way or other give an idea of its sources, methods and/or its current level of knowledge. The Committee observes in this context that it follows from the explanatory memorandum to article 6 of the Classified Information Security

Regulations, that if only one passages contains state secret information, the entire document must be classified as state secret. It is therefore the opinion of the Committee that in by far the most cases the state secret classification of operational information was in conformity with legislative and regulatory provisions. (section 7)

13.14 The Committee has established that GISS classifies as state secret both the use of special powers in specific cases and the circumstances connected with such use, e.g. the operational parameters. The Committee considers this to be in conformity with the legislative and regulatory rules. (section 7.1.1)

13.15 The Committee holds the opinion that a multi-year overview of tap statistics cannot be considered state secret information. (section 7.1)

13.16 In addition to the concrete use of special powers GISS also classifies other operational assessments and characteristics of an investigation as state secret information. Examples are the designation of targets, action plans, team assignments and prioritizations, exploitation policy and the details of cooperation with foreign counterparts. The Committee holds the opinion that such data, which relate to methods for the secret collection of operational information, are rightly classified as state secret. (section 7.1.1)

13.17 The Committee observes that there are bounds to the possibility of designating a method as state secret information. It holds the opinion, for example, that this requires an up-to-date, unknown method. Its unknownness can lie in the person with respect to whom the method is used, or be connected in a general sense to the method itself being unknown, for example in connection with the technical capacities of the service. In the opinion of the Committee the necessity to keep secret the methods used by GISS is in all cases subject to erosion by the mere lapse of time. (section 7.1.1)

13.18 The Committee holds the opinion that GISS generally classified information relating to human sources as state secret in conformity with the legislative and regulatory rules. (section 7.1.2)

13.19 The Committee observes that the necessity to protect sources, and therefore the necessity to classify, depends on the context in which the information was provided to GISS. The covert nature of contacts between source and GISS employee is particularly relevant here. The Committee has established that GISS also classifies as state secret reports of meetings in connection with the performance of its security-promoting task pursuant to article 6(2)(c) ISS Act 2002. The Committee holds the opinion that the state secret nature of such meetings is far from evident. (section 7.1.2)

13.20 GISS finds a connection between breaches of professional integrity within GISS and their supposed negative influence on the willingness of (future) sources to provide information to GISS. The Committee holds the opinion that such a connection should not be assumed too readily and that a categorical refusal to allow an application for inspection of files on the grounds of source protection is not in conformity with the legislative and regulatory rules. (section 7.1.2)

13.21 The Committee holds the opinion that the notification forms sent by the Regional Intelligence services to GISS pursuant to article 62 ISS Act 2002 are often wrongly classified as state secret. The Committee holds the opinion that the mere fact that

information is communicated to GISS does not by definition mean that it is state secret information. (section 7.1.2)

13.22 The Committee holds the opinion that GISS generally implements the classification of information relating to current level of knowledge correctly. (section 7.1.3)

13.23 The Committee has established that GISS assigns state secret classification to certain analyses of the regular media. It did so to a collection of relevant media reports without linking them to specific operational investigations. The Committee holds the opinion that classifying this information as state secret is not in accordance with the legislative and regulatory rules. (section 7.1.3)

13.24 The Committee holds the opinion that in the case of official messages issued to the ministry of Economic Affairs, Agriculture and Innovation the general interest of national security must outweigh the individual interest which the exporter concerned has in examining the official messages. (section 7.2.1)

13.25 In by far the most cases the Committee holds the opinion that GISS rightly classified as state secret the Short Information Reports and Special Intelligence Analyses it issued. In a few cases the Committee holds the opinion that GISS could not reasonably have taken the decision to classify the reports as state secret. The Committee holds the opinion that the purport of the reports in question is so general that they cannot reasonably be classified as state secret. In those cases, moreover, it may be assumed that it was quite well-known that GISS was investigating the countries in question. (section 7.2.2)

13.26 **The Committee recommends that GISS, where necessary, states in a document that even though a report does not contain state secret content, it must nevertheless be classified as state secret because of its investigation subject.** (section 7.2.2)

13.27 The Committee draws attention to the fact that one single passage containing state secret information will have the result that the entire document must be classified as state secret. **The Committee recommends that where possible GISS states in such cases for each paragraph whether it is state secret.** (section 7.2.2)

13.28 The Committee holds the opinion that in general the products in the context of the Surveillance and Protection System are correctly classified as state secret. It has established that in the case of threat and risk analyses GISS adopted at least the classification level of the application of the Surveillance and Protection Coordinator. The Committee considers this to be the correct basic principle. If the nature of the information gives cause to do so, it can be classified at a higher level. The Committee holds the opinion that in the cases in which GISS assigned a higher level it rightly decided to do so. (section 7.2.3)

13.29 The Committee holds the opinion that the Surveillance and Protection System products issued on the initiative of GISS (threat reports or threat assessments) were in general rightly classified as state secret. In respect of a number of threat reports the Committee holds the opinion that state secret classification is not necessary. In the opinion of the Committee the mere fact that the threat report contains the assessment of GISS without this being traceable to state secret sources or without revealing the

actual level of knowledge, does not constitute sufficient grounds to classify the report as state secret. (section 7.2.3)

13.30 The Committee holds the opinion that Surveillance and Protection System products, particularly threat reports, are eminently suitable for being made subject to a classification expiry date that is linked to a specific event. Article 6(1) of the Classified Information Security Regulations expressly provides for this possibility. In many cases the threat report mentions an increased threat around a certain event. The Committee holds the opinion that in such cases the classification can be linked to how the event develops. (section 7.2.3)

13.31 The Committee holds the opinion that internal reports in the context of the security-promotion task should not be automatically classified as state secret because these reports are intended for internal use only. The same applies to internal reports of background interviews with journalists, concerning publications by GISS for example. (section 7.2.4)

13.32 The Committee has established that GISS also assigns state secret classification to other external contacts, for example reports received at the front office of GISS and reports of general consultations with third parties. The Committee holds the opinion that in many cases there is no necessity for such classification and recommends that GISS will not classify such information if it is not necessary. (section 7.2.4)

13.33 The Committee holds the opinion that GISS usually decides in a correct manner not to inform the person concerned of certain information in connection with a refusal to issue a certificate of no objection, because the refusal is based on the state secret nature of the information. In the cases in which GISS refrained from mentioning state secret information, the Committee holds the opinion that GISS classified this information as state secret on correct grounds. (section 7.3)

13.34 The Committee holds the opinion that screening reports are rightly classified as state secret, even if they do not include information obtained from sources. (section 7.3)

13.35 The Committee has established that where the personal data of an intended holder of a confidential position are linked to the specific position, this information is classified as state secret. The Committee holds the opinion that this is hardly consistent with the unclassified "Screening Application Form" which is filled out by the employer of the person concerned and on which he fills out this information as well. (section 7.3)

Classification of other information

13.36 The Committee has established that in many cases GISS classified as state secret information relating to the personnel policy at GISS. The Committee has established that it concerns information that is not unique for an organisation like GISS. The Committee holds the opinion that in many cases it can be doubted whether it is necessary to classify this type of information as state secret. (section 8.1)

13.37 The Committee holds the opinion that in a number of cases GISS wrongly classified legal memorandums as state secret. (section 8.2)

Classification levels

13.38 Information reports are classified state secret - CONFIDENTIAL, unless there are operational reasons for using a higher classification level. In that case an internal guideline at GISS requires that the assessment leading to the higher classification level must be recorded in a retrievable manner. The Committee has established that in many cases no such assessment record exists. **It recommends that GISS ensures that such records are kept.** (section 9.2)

13.39 The Committee has established that there are some operational reports from which the identity of the source can be inferred. The Committee holds the opinion that this is inconsistent with the very stringent view of source protection taken at GISS. The Committee holds the opinion that such information should only be mentioned in the agent source file and recommends that GISS ensures that this is the case. The Committee holds the opinion that all information that can be traced back (directly) to the source must be stored in the agent source file. If it is necessary to include the information in the operational report, the classification of the operational report must be adjusted. (section 9.2)

13.40 A number of the persons interviewed said that they used a higher classification level to prevent (too) wide distribution of the information *within GISS* or to prevent end users of a GISS product from being careless about handling the security regulations. The Committee holds the opinion that this means that the information is classified at too high a level. The appropriate means for preventing information from being too widely distributed within GISS is to take adequate measures limiting access to the information and not the use of higher classification levels. **The Committee recommends that GISS enshrines this principle in its internal regulations.** (section 9.3)

13.41 The Committee has found that in many cases the default classification in the template is viewed as an established fact. The Committee holds the opinion that it must be assessed for each individual document what is the appropriate classification level and that the default classification can be no more than an indication. The classification of the document must be determined on the basis of the information included in the document. It is the opinion of the Committee that there is insufficient evidence that such individual assessments take place. (section 9.4)

13.42 The Committee has established that in many cases there is a high degree of similarity between the reasons stated in the application for permission to wiretap and the reasons stated for obtaining telephone traffic data with respect to the same person or organisation. In the opinion of the Committee the fact that the reasons for using a telephone tap are mentioned cannot give cause for applying a different classification level than the classification level assigned to the substantiated application for telephone traffic data. The Committee therefore holds the opinion that in this respect the classification is inconsistent and recommends that GISS remedy the inconsistency. **The Committee recommends addressing this issue in the classification guidelines to be drafted.** (section 9.4)

13.43 **The Committee recommends linking the classification level of the use of special powers to the necessity of keeping secret the investigation of a specific person, organisation or phenomenon**. For certain investigation subjects this necessity will be

greater and will therefore necessitate a higher classification level. All special powers used in respect of a specific investigation subject will have to be classified at the same level. This principle means that it is not the nature of the special powers that will affect the classification level, but only the subject in respect of whom or which the special power is used. (section 9.4)

13.44 **The Committee recommends that GISS starts consulting with DISS about the practical problems entailed by handling Sigint/Comint information.** (section 9.4)

Destruction and declassification

13.45 The Committee recognizes the great importance of protecting the human sources of GISS. The Committee holds the opinion, however, that a categorical refusal to transfer agent and informer files to the National Archives lacks a legal basis. The Committee holds the opinion that GISS may be required to assess on a case-by-case basis whether the interest of source protection prevents transfer to the National Archives. The Committee does not exclude that in some cases the interest of source protection no longer plays a role in transferring files to the National Archives. In general, the Committee considers a twenty-year ban on transferring agent and informer files to be relatively short. In many cases disclosure of the relationship with GISS may still endanger the safety of human sources, which bars disclosure of these data. After a period of 75 years, however, the Committee believes this to be conceivable only in very rare cases. **It recommends that GISS further examines the possibility of transferring files in a fully anonimized form, in conformity with a proposal to such effect of the minister of Education, Culture and Science.** (section 10.1)

13.46 The Committee has established that in actual practice GISS does not have a structural *active* declassification programme in place. The Committee holds the opinion that GISS is thus acting contrary to the Classified Information Security Regulations, article 44 ISS Act 2002, and its internal regulations. (section 10.2)

13.47 The Committee has examined a closed investigation by GISS which has not yet been the subject of an application for inspection and in respect to which the possibility of declassification has not yet been examined. The Committee holds the opinion that the information included in such files can in many cases be declassified without any problems. (section 10.2)

13.48 The Committee holds the opinion that GISS, when processing applications for inspection of files, can pursue greater openness particularly in the matter of declassifying the methods used in the past by the legal predecessor(s) of GISS. (section 10.2.)

13.49 The Committee recognizes that it is not inconceivable that an information report will give an idea of the identity of the source. Operational reports in particular are likely to do so. In such cases GISS will have to be careful about declassifying the information or refrain from declassification. The Committee holds the opinion that GISS must assess on a case-by-case basis whether the data in question considered separately or in combination with each other give an idea of the identity of the source. (section 10.2)

13.50 Based on the selection list serving as a basis for transferring or destroying files GISS can establish which data are to be destroyed and which records will eventually be eligible for transfer. In the opinion of the Committee it will not be necessary to examine whether data earmarked for destruction can be declassified. (section 10.3)

13.51 **The Committee recommends paying more up-front attention to the temporal nature of classification and the grounds on which the decision to classify information as state secret was taken.** (section 10.3)

13.52 **The Committee considers it advisable for GISS to structure the preparation of records in such a way as to anticipate at this early stage, where possible, the transfer or destruction of the elements of the records about which there is agreement between the ministry of the Interior and Kingdom Relations and the ministry of Education, Culture and Science**. (section 10.3.)

Permanent Parliamentary Committee on Intelligence and Security Services (Permanent ISS Committee)

13.53 **The Committee recommends that where possible GISS states for each individual paragraph of all information provided to the Permanent ISS Committee whether it is state secret.** (section 11)

13.54 The picture obtained by the Committee is that the information from GISS provided to the Permanent ISS Committee was in most cases rightly classified as state secret information. In a number of cases it is the opinion of the Committee that the state secret classification was not necessary. (section 11)

13.55 The Committee holds the opinion that in two cases a memo of an interview with a chairperson of a political group in the Second Chamber was wrongly classified as state secret. (section 11)

13.56 In the opinion of the Committee a letter concerning the ongoing discussion about the selection lists between GISS and DISS on the one hand and the National Archives of the other has been wrongly classified as state secret. The letter merely sets out the legal framework for source protection by GISS and further mentions the transfer or destruction, respectively, of certain data. (section 11)

13.57 The Committee holds the opinion that the covering letter concerning the screening of the antecedents of (candidate) political office holders was wrongly classified as state secret. (section 11)

13.58 The Committee holds the opinion that information that has been provided to the Public Prosecution Service in a public official message has thereby been declassified. This means that it is unnecessary to classify as state secret the information presented to the Permanent ISS Committee. (section 11)