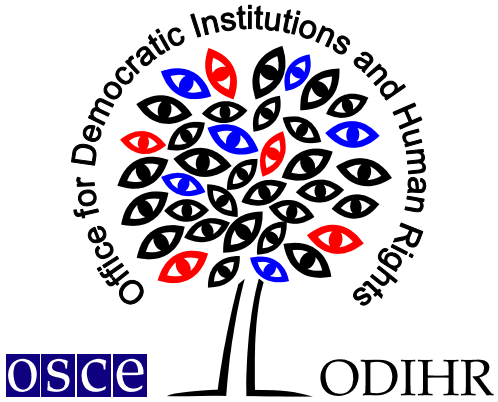
Warsaw, 12 October 2009 Opinion-Nr.: FOI – SRB/141/2009 www.legislationline.org	

Comments
on The Draft Law
of The Republic of Serbia
on Secrecy of Information

based on an English translation of the draft law provided by the OSCE Mission to Serbia

These Comments have been prepared by Irina Urumova, OSCE/ODIHR Expert

TABLE OF CONTENTS:

1. INTRODUCTION

1. *On 26 August 2009, the OSCE/ODIHR was requested by the OSCE Mission to Serbia to review the draft Law of the Republic of Serbia on Secrecy of Information. The request is a follow-up to the Mission´s support to the working group on drafting the law in question, undertaken at the request of the Ministry of Justice of January 2009.*

2. *The Comments contained herein (hereinafter referred to as "the Comments") have been drafted in response to the above request for assistance.*

2. SCOPE OF REVIEW

3. The scope of the Comments covers only the draft Law of the Republic of Serbia on Secrecy of Information (hereinafter referred to as "draft Law" or "Draft"), which was submitted for review. Therefore, the Comments do not constitute a full and comprehensive review of all available framework legislation governing the issue in the Republic of Serbia. Instead, these Comments analyze the Draft from the viewpoint of its compatibility with relevant international human rights standards and OSCE commitments. The Comments also examine the draft Law in light of international good practices with regard to access to information, national security and official secrecy laws.

4. The Comments are based on an unofficial translation of the text of the Draft provided by the OSCE Mission to Serbia. Errors from translation may result.

5. The OSCE/ODIHR would like to mention that the recommendations provided herein are without prejudice to any further comments, opinions or recommendations that the ODIHR may wish to make on the issue under consideration.

3. EXECUTIVE SUMMARY

6. Legislation on official secrecy needs to balance security interests against the need to ensure full protection of the public´s right of knowledge. It is essential that information classified as state secrets be narrowly defined and that access to information be only restricted where the data at issue directly relate to national security and where their disclosure to unauthorized parties would pose an identifiable and serious threat. Certain information, such as information related to human rights violations, public health and environmental hazards, administrative errors, and other information of public interest, should not be eligible for classification under any circumstances.

7. The draft Law in question poses a number of concerns due to the vagueness of some of its key provisions and the sweeping categorization of information classifiable as state secret. It does not single out categories of information that are not eligible for classification. Moreover, the provisions that allow the refusal of access to classified data, albeit on an exceptional and temporary basis, to representatives of oversight agencies, seriously undermine the efficiency and effectiveness of oversight mechanisms envisaged under the Draft. It is recommended that the draft Law be revised to eliminate vagueness and to ensure specificity, to provide for categories of information of public interest that cannot be classified under any circumstances, and to put in place a viable oversight mechanism.

8. The full list of recommendations follows below.

A. The definition of classifiable information under the draft Law in question is overly broad and vague. It is recommended that the definition be revised in the

interests of clarity and specificity. Additionally, the phrase "*protection of the interests of the Republic of Serbia*" is recommended to be replaced with a narrowly defined purpose limiting the application of the law to such information that would harm national security if disclosed. It is also strongly recommended that the reference to "*protection of ... human rights and freedoms*" be removed from the definition of "*data of the interest for the Republic of Serbia*". *[Articles 2 and 8, discussed in para. 11]*

B. It is strongly recommended that the draft Law provide for a detailed list of categories of information eligible for classification, and that it narrowly delineate the scope of each category. *[Article 8, discussed in par. 12]*

C. The provision that classified information may only be used for the purposes it was collected for, in accordance with the law, is welcome. *[Article 5, discussed in par. 13]*

D. It is strongly recommended that the draft Law expressly prohibit the classification of certain categories of information, most importantly information related to human rights violations, public health and environmental hazards, and administrative errors. Liability for classifying such information in contravention of the law should be included in the Draft. *[Throughout the Draft, discussed in pars. 14-17]*

E. It is recommended that specific provisions be introduced to ensure protection for whistleblowers. In this context, it is recommended that the requirement for anyone aware of the contents of classified information to maintain its secrecy, "regardless of the manner of learning such information" be revised to specifically exempt whistleblowers. *[Article 6, discussed in par. 18]*

F. It is recommended that the category of information classified as "restricted" be excluded from the scope of the draft Law. If necessary, the legislation on access to information may be amended to regulate "restricted"-level information. *[Article 14, discussed in par. 19 and 20]*

G. It is recommended that the draft Law be revised to vest comprehensive oversight powers in the authorized oversight body, including the power to review secrecy levels and to order declassification of information. Such oversight body should enjoy unimpeded access to classified information. *[Article 40, discussed in par. 21-24]*

4. ANALYSIS AND RECOMMENDATIONS

4.1 Definition of Classified Information and Rationale for Classification

9. The draft Law permits classification of any "*data of interest to the Republic of Serbia*" if their disclosure is likely to "*cause damage, if the necessity of protection the interests of the Republic of Serbia prevails over the interest in free access to information of public importance.*"[1] The Draft defines "*data of interest to the Republic of Serbia*" as "*any information or document at the disposal of public authorities, which relates to territorial integrity and sovereignty, protection of constitutional system and human rights and freedoms, national and public security, defence, internal and foreign affairs.*"[2] The draft Law specifies four broad categories of classifiable data, namely those concerning " *1) the national security of the Republic of Serbia, public security, namely defence, foreign policy, security and intelligence affairs of the public authorities; 2) the relations of the Republic of Serbia with other countries, international organizations and other international entities; 3) systems, devices, projects, plans and structures related to the data mentioned in items 1 and 2 of this paragraph; 4) scientific, research, technological, economic and financial affairs related to the data mentioned in items 1 and 2 of this paragraph.*"[3]

10. While legislation on what constitutes "official secrets" plays a prominent role in protecting national security, and while the protection of national security under international human rights law can be invoked as a ground to impose restrictions on freedom of access to information,[4] it is essential that information classified as state secrets be narrowly defined and that access to information only be restricted where the data in question directly relate to national security and where their disclosure to unauthorized parties would pose an identifiable and serious threat. This principle was voiced by the OSCE Representative on Freedom of the Media[5] as a core standard that national legislation on official secrecy of OSCE participating States has to comply with. Furthermore, Recommendation 1792 (2007) of the Parliamentary Assembly of the Council of Europe (CoE) specifically called on the CoE member States to "*[e]xamine existing legislation on official secrecy and amend it in such a way as to replace vague and overly broad provisions with specific and clear provisions, thus eliminating any*

---

1 See Article 8 of the Draft Law on Secrecy of Information (Annex A hereto)

2 *Id.*, Article 2

3 *Id.*, Article 8.

4 International Covenant on Civil and Political Rights (ICCPR), Article 19(3) ("*The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (*ordre public*), or of public health or morals.*"); European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), Article 10(2) ("*The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.*"). Serbia is a State Party to both the ICCPR (by succession, as of 12 Mar 2001) and the ECHR (ratified on 3 March 2004). Full texts of the treaties are available on the web at: http://www2.ohchr.org/english/law/ccpr.htm (ICCPR) and http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm (ECHR).

5 OSCE Representative on Freedom of the Media, Access to information by the media in the OSCE region: Trends and Recommendations: Summary of Preliminary Results of the Survey, 30 April 2007 ("*The definition of state secrets should be limited only to data that directly relate to the national security of the state and where their unauthorized release would have identifiable and serious consequences.*")

risks of abuse or unwarranted prosecutions."[6] The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights further specify that "*[n]ational security may be invoked to justify measures limiting certain rights only when they are taken to protect the existence of the nation or its territorial integrity or political independence against force or threat of force*[7]."

11. The definition of classifiable information under the draft Law in question is overly broad and vague, and as such does not comply with the relevant international standards. It also runs counter to the fundamental principle of legality, which requires that all law be clear and ascertainable, and that consequences of a breach be foreseeable. It is recommended that the definition of classifiable information be revised for better clarity and specificity, and that "*protection of the interests of the Republic of Serbia*" be replaced with a narrowly defined purpose limiting the application of the draft Law to such information that would harm national security if disclosed. It is also strongly recommended that the reference to "*protection of ... human rights and freedoms*" be removed from the definition of "*data of interest to the Republic of Serbia.*"

12. It is strongly recommended that the law provide for a detailed list of categories of information eligible for classification, and that it narrowly delineate the scope of each category. The drafters may wish to use Estonia´s State Secrets Act[8] and Poland´s Classified Information Protection Act as sources for inspiration.[9]

13. At the same time, the provision in the draft Law that classified information may only be used for the purposes it was collected for, in accordance with the law,[10] is welcome and consistent with the requirements of the European Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data that data be "*stored for specified and legitimate purposes and not used in a way incompatible with those purposes.*"[11]

---

[6] Parliamentary Assembly of the Council of Europe, Recommendation 1792 (2007) Fair trial issues in criminal cases concerning espionage or divulging state secrets, §1.1.1.

[7] U.N. Doc. E/CN.4/1985/4, Annex (1985), Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, Principle 29.

[8] See Annex B hereto.

[9] See Annex C hereto.

[10] See Article 5 of the Draft Law on Secrecy of Information

[11] European Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Article 5 ("*Personal data undergoing automatic processing shall be: a. obtained and processed fairly and lawfully; b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes.*")

4.2 Information Prohibited from Classification

14. The draft Law does not provide for information that is not eligible for classification. In combination with the overly broad definition of classifiable information that includes a reference to "*protection of ... human rights and freedoms*," this creates a risk of arbitrary and potentially abusive implementation, whereby access to information of public interest may be restricted.

15. Prohibiting the classification of information which is of public interest is key to democratic governance and the respect for human rights. The categories of information that cannot be classified under any circumstances typically include information related to human rights violations, public health and environmental hazards, and administrative errors.

16. The OSCE Representative on Freedom of the Media has urged the participating States against classifying "*[i]nformation relating to violations of the law or human rights, maladministration or administrative errors, threats to public health or the environment, the health of senior elected officials, statistical, social-economic or cultural information, basic scientific information, or that which is merely embarrassing to individuals or organisations.*"[12] The UN Working Group on Arbitrary Detention has recommended that "*Governments take all necessary measures, of a legislative or other nature, to ensure that any legislation and regulations concerning national or State security should in no case be extended to cover information relating to the protection either of the environment or of human rights standards*."[13] The UNECE Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters (Aarhus Convention) imposes a positive obligation on State Parties to immediately disseminate to the public all relevant information held by the government in the event of any imminent threat to human health or the environment.[14] The prohibition on classifying information related to public health or environmental hazards is implicit in this requirement.

17. It is strongly recommended that the draft Law expressly prohibit the classification of certain categories of information, most importantly information related to human rights violations, public health and environmental hazards, and administrative errors. Liability for classifying such inherently open information in contravention to the law should be included in the Draft. As far as good practices from OSCE participating States are concerned, the drafters may draw inspiration from Latvia´s Law on Official Secrets[15] and Ukraine´s Law on State Secret.[16]

---

[12] OSCE Representative on Freedom of the Media, Access to information by the media in the OSCE region: Trends and Recommendations: Summary of Preliminary Results of the Survey, 30 April 2007.

[13] UN Working Group on Arbitrary Detention, Recommendation: Human Rights and State Secrets, E/CN.4/2001/14, 20 December 2000.

[14] UNECE Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters, Article 5(1)(c) ("*In the event of any imminent threat to human health or the environment, whether caused by human activities or due to natural causes, all information which could enable the public to take measures to prevent or mitigate harm arising from the threat and is held by a public authority is disseminated immediately and without delay to members of the public who may be affected.*"). Serbia acceded to the Convention on 31 July 2009. Full text of the Convention is available on the web at http://www.unece.org/env/pp/documents/cep43e.pdf.

[15] Latvia, Law on Official Secrets, Section 5 ("*It is prohibited to grant the status of an official secret and to restrict access to the following information:*

1) information regarding natural disasters, natural or other calamities and the consequences thereof;

2) information regarding the environmental, health protection, educational and cultural state, as well as the demographic situation;

3) information regarding violations of human rights;

18. It is also recommended that the prohibition on the classification of certain categories of information be reinforced by specific provisions ensuring whistleblower protection. Such provisions would apply to persons (whistleblowers) who release classified information that is of significant public interest. In this connection, it is recommended that the requirement for anyone aware of the contents of classified information to maintain its secrecy, "*regardless of the manner of learning such information*" be revised to specifically exempt whistleblowers.[17]

4) information regarding the crime rate and the statistics thereof, corruption cases, irregular conduct of officials;

5) information regarding the economic situation in the State, implementation of the budget, living standards of the population, as well as the salary scales, privileges, advantages and guarantees specified for officials and employees of State and local government institutions; and

6) information regarding the state of health of the heads of State.")

[16] Ukraine, Law on State Secret, Article 8 ("*It is prohibited to refer to state secret any data, if it may cause constriction of content and volume of constitutional rights and freedoms of a person and citizen, or if it may harm health and safety of a person.*

The following information may not be referred to state secret:

- on state of environment, on quality of food and household goods;

- on accidents, catastrophes, dangerous natural phenomena and other extraordinary events, which occurred or may occur and threaten citizens' security;

- on health state of population, its living standard, including meals, cloths, accommodations, medical care and social security, as well as on social-demographic showings, level of legal order, education and culture of population;

- on facts of violation of rights and freedoms of a person and citizen;

- on illegal actions of governmental bodies, local authorities and their officials;

- other information, which according to laws and international agreements, obligation of which is provided by Verkhovna Rada of Ukraine, may not be classified.")

[17] See Article 6 of the Draft Law on Secrecy of Information

4.3 Designation of Secrecy Level

19. The draft Law, in accordance with Article 1 thereof[18], is essentially a law on state secrets. The Draft provides for four levels of state secrets: top secret, secret, confidential and restricted.[19] While the first 3 levels are overall consistent with relevant international standards and the body of good practice, the "restricted" level of information (defined as "*determined in order to prevent the occurrence of damage for the work, namely for the performance of assignments and jobs of the public authority that had defined it*")[20] is essentially what is commonly known as an "official secret," and as such should be regulated by access to information legislation rather than by a law on state secrets. This view has been endorsed by the OSCE Representative on Freedom of the Media who has recommended that "*[i]nformation designated as "official" or "work secrets" should not be considered for classification as state secrets. Limits on their disclosure should be found in the access to information law.*"[21]

20. It is recommended that the category of information classified as "restricted" be excluded from the scope of the draft Law. If necessary, the Serbian legislation on access to information may be amended to regulate "restricted"-level information.

4.4 Oversight

21. The draft Law designates the Office of the National Council for Security and Protection of Classified Information as the oversight body with the power to order declassification.[22] At the same time, the draft Law allows the restriction of access by representatives of oversight bodies, albeit exceptionally and temporarily, to information classified as "top secret" and/or "secret." The bodies in question are the Office of the National Council for Security and Protection of Classified Information as well as the Ombudsperson and the Commissioner for Access to Information of Public Importance and Protection of Personal Data.[23] The authorized holder of classified information at issue is the only body entitled to make decisions on restricted access. In the event that the oversight body disagrees with the decision of the holder of such information, it may request the initiation of internal review and/or appeal the decision in court.[24]

22. The possibility of restricting access for oversight bodies raises especially serious concerns, as it effectively undermines checks and balances in the classification policy. The existence of an independent oversight body with the power of monitoring classification and ordering redesignation of secrecy levels and/or declassification of information is key to preventing an arbitrary implementation of secrecy laws.

23. OSCE participating States have accumulated an ample body of good practice with regard to secrecy oversight that may be used for reference and inspiration. For instance, Norway´s Act relating to Protective Security Services provides the oversight body with "*unhampered access to any area where there is sensitive information or a sensitive object, if the area is*

---

18 *Id.*, Article 1

19 ***Id.*, Article 14**

20 *Id.*

21 OSCE Representative on Freedom of the Media, Access to information by the media in the OSCE region: Trends and Recommendations: Summary of Preliminary Results of the Survey, 30 April 2007.

22 See Article 24 of the Draft Law on Secrecy of Information, Article 24

23 *Id.*, Article 40

24 *Id.*

owned, used or otherwise controlled by an enterprise."[25] In the United States, the Information Security Oversight Office (ISOO) is the federal agency responsible for the comprehensive oversight of the Government-wide security classification system and the national Industrial Security Program. ISOO is mandated (a) to develop security classification policies for classifying, declassifying and safeguarding national security information; (b) to evaluate the effectiveness of the security classification programs; and (c) to develop standardized controlled unclassified information policies and procedures that appropriately protect sensitive information through effective data access and control measures. ISOO has the power to order declassification of information.[26] Additional safeguards in respect of public accountability of secrecy are provided by the Public Interest Declassification Board, which is an advisory committee established by the United States Congress with the official mandate of promoting the fullest possible public access to a thorough, accurate, and reliable documentary record of significant U.S. national security decisions and activities.

24. It is recommended that the draft Law be revised to vest comprehensive oversight powers in the authorized oversight body, including the power to review secrecy levels and to order declassification of information. Such an oversight body should enjoy unimpeded access to classified information.

[END OF TEXT]

[25] Norway, Act of 20 March 1998 No. 10 relating to Protective Security Services, Section 19 ("*Insofar as is necessary for implementing the supervisory functions laid down in or pursuant to this Act, the National Security Authority shall be given unhampered access to any area where there is sensitive information or a sensitive object, if the area is owned, used or otherwise controlled by an enterprise.*")

[26] Executive Order 13292—Further Amendment to Executive Order 12958, as Amended, Classified National Security Information, Section 3.1(c) ("*If the Director of the Information Security Oversight Office determines that information is classified in violation of this order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the President through the Assistant to the President for National Security Affairs. The information shall remain classified pending a prompt decision on the appeal.*")

ANNEX A: Draft Law of the Republic of Serbia on Secrecy of Information

DRAFT

THE LAW
ON
SECRECY OF INFORMATION

I. GENERAL PROVISIONS

Subject of the Law

Article 1

This law prescribes the uniform system of classification and protection of classified information, which are of interest for the national and public security, defence, internal and foreign affairs of the Republic of Serbia, protection of foreign classified information, access to classified information and termination of their secrecy, competence of authorities and supervision of enforcement of this law, as well as the responsibility for non-fulfilment of obligations prescribed by this law and other issues of importance for the protection of information secrecy.

Expressions

Article 2

Within the meaning of this law:

1) *information of the interest for the Republic of Serbia* is any information or document at the disposal of public authorities, which relates to territorial integrity and sovereignty, protection of constitutional system and human rights and freedoms, national and public security, defence, internal and foreign affairs;

2) *classified information* is the information of the interest for the Republic of Serbia, which has been classified or identified to have a certain level of secrecy by law, other regulation or decision of the competent body adopted pursuant to law;

3) *foreign* classified *information* is the information entrusted to the Republic of Serbia by a foreign country or an international organization under the provision it shall be kept secret, as well as the classified information resulting from the co-operation between the Republic of Serbia and other countries, international organizations and other international entities, in compliance with the international treaty concluded between the Republic of Serbia and a foreign country, international organization or other international entity;

4) *document* is any information holder (paper, magnetic or optical media, diskette, USB memory, smart card, compact disc, microfilm, video and audio records, etc.), on which classified information has been recorded or memorized;

5) *determination of classified information* is the procedure in which some information is determined to be classified, in accordance with this law, also defining the level and duration of secrecy;

6) *designation of secrecy level* is marking of classified information with the following: TOP SECRET , SECRET, CONFIDENTIAL or RESTRICTED;

7) *public authority* is a state body, a body of territorial autonomy, a body of local self-government, an organization entrusted with the exercise of public powers, as well as a legal entity established by the state body or which is financed either entirely or the prevailingly from the budget, which deals with classified information, namely the one

generating, obtaining, keeping, using, exchanging or processing classified information in some other way;

8) *security checkout* is the procedure conducted by the competent body before the issuance of the approval for access to classified information, in order to collect the data about the possible security risks and disturbances in respect of reliability for the access to classified information;

9) *damage* is a violation of the interests of the Republic of Serbia resulting from an unauthorized access, disclosure, spoliation and abuse of classified information or resulting from some other action of classified information processing and foreign classified information processing;

10) *operator of classified information* is a natural person or an organizational unit of public authority, which undertakes measures for the protection of classified information in accordance with the provisions of this law (hereinafter referred to as the operator);

11) *user of classified information* is a citizen of the Republic of Serbia or a legal entity having the seat in the Republic of Serbia, which has been granted an approval by the competent body, namely a foreign natural person or a legal entity, which has been granted a security permit for the access to classified information (hereinafter referred to as the permit) on the grounds of the concluded international treaty, as well as an official of the public authority who, pursuant to this law, has the right to access and use classified information without the issuance of the approval;

12) *security risk* is an actual possibility of violation of classified information security;

13) *protective measures* are general and special measures undertaken in order to prevent the occurrence of damage, namely the measures related to the accomplishment of administrative, information-telecommunication, personal and physical security of classified information and foreign classified information.

Information not Considered Classified Information

Article 3

Classified information is not considered classified if it has been identified as classified in order to conceal a criminal act, transgression of powers or abuse of official duty or other illegal act or actions by the public authority.

Access Right

Article 4

The access to classified information is possible in the manner and under the conditions established by this law, regulations adopted on the grounds of this law and international treaties.

Purpose of Collection

Article 5

Classified information may only be used for the purposes they had been collected for, according to the law.

Keeping and Use

Article 6

Classified information are kept and used in accordance with the protective measures prescribed by this law, regulation adopted on the grounds of this law and international treaties. A person using classified information or a person having learned its contents is obliged to protect such information regardless of the manner of learning such information.

The obligation referred to in paragraph 2 of this Article also remains in force after the termination of duty or employment, namely after the termination of the performance of duty or the membership in the relevant body.

Protection of Business and Other Secrets

Article 7

Protection of business and other secrets is governed by separate laws.

II. DETERMINATION OF CLASSIFIED INFORMATION

Information that Might be Determined as Classified Information

Article 8

Any data of the interest for the Republic of Serbia may be determined as classified information whose disclosure to an unauthorized person would cause damage, if the necessity of protection of the interests of the Republic of Serbia prevails over the interest for free access to information of public importance.
The data referred to in paragraph 1 of this Article particularly concern:
1) the national security of the Republic of Serbia, public security, namely defence, foreign policy, security and intelligence affairs of the public authorities;
2) the relations of the Republic of Serbia with other countries, international organizations and other international entities;
3) systems, devices, projects, plans and structures related to the data mentioned in items 1 and 2 of this paragraph;
4) scientific, research, technological, economic and financial affairs related to the data mentioned in items 1 and 2 of this paragraph.

Person Authorized to Determine Classified Information

Article 9

An authorized person is to determine classified information under the conditions and in the manner established by this law.
The authorized persons are:
1) the President of the National Assembly;
2) the President of the Republic;
3) the Prime Minister;
4) the head of the public authority;
5) an elected, appointed or nominated official of the public authority authorized to determine classified information by law, namely by the regulation adopted on the grounds of law, or who has been authorized to do so by the head of the public authority in writing;
6) a person employed with the public authority who has been authorized to do so by the head of the public authority in writing.
The authorized persons referred to in paragraph 2, items 5 and 6 of this Article may not transfer their authorizations to other persons.

Procedure to Determine Classified Information

Article 10

The authorized person referred to in Article 9 paragraph 2 of this law determines classified information on the occasion of its occurrence, namely when the public authority starts to perform the job resulting in the occurrence of classified information.
As an exemption from paragraph 1 of this Article, the authorized person may also determine classified information subsequently, after the criteria defined by this law had been fulfilled.

During the determination of classified information, the authorized person assesses possible damage for the interests of the Republic of Serbia.
A person employed with the public authority, namely a person performing certain jobs with the public authority is obliged, within the framework of his/her assignments, namely within the framework of authorizations, to inform the authorized person about the information that might be determined as classified information.

Decision on Determination of Secrecy Level

Article 11

The decision on determination of secrecy level is adopted on the basis of the evaluation referred to in Article 10 paragraph 3 of this law, and accordingly, the documents are marked with secrecy level as prescribed by this law (hereinafter referred to secrecy designation).
During the determination of secrecy level of information the authorized person identifies the lowest level of secrecy preventing the occurrence of damage for the interests of the Republic of Serbia.
If a document contains information that might be designated with different levels of secrecy, the authorized person designates the document with a higher level of secrecy in relation to such secrecy levels.
The decision referred to in paragraph 1 of this Article is adopted in the written form, including the statement of reasons.

Special Cases of Determination and Designation of Classified Information

Article 12

The authorized person shall determine as classified the information resulting from the consolidation or linking the information that are not classified information by themselves, if the information consolidated or linked in such a way present the information that need to be protected for the reasons established by this law.
The document containing already classified information with different levels of secrecy and secrecy holding, is determined to have a higher level of secrecy and longer keeping of secrecy of the contained information in relation to such information.
If a minor part of the document contains classified information, it is separated and attached as a separate enclosure marked with secrecy level.

Secrecy Designations

Article 13

The document containing classified information is marked with:
1) the designation of secrecy level;
2) the method of termination of secrecy;
3) the data about the authorized person;
4) the data about the public authority.

As an exemption from paragraph 1 of this Article some information are considered classified information if the document containing the information is only designated with secrecy level.
The Government prescribes the method and the procedure of determination of classified information, namely the documents.

Secrecy Level and Contents of Information

Article 14

The information referred to in Article 8 of this law may have one of the following secrecy levels:
1) TOP SECRET, which is determined in order to prevent the occurrence of irreparable damage for the interests of the Republic of Serbia;

2) SECRET, which is determined in order to prevent the occurrence of severe damage for the interests of the Republic of Serbia;
3) CONFIDENTIAL, which is determined in order to prevent the occurrence of damage for the interests of the Republic of Serbia;
4) RESTRICTED, which is determined in order to prevent the occurrence of damage for the work, namely for the performance of assignments and jobs of the public authority that had defined it.

Secrecy levels referred to in paragraph 1 of this Article may only be used to determine secrecy levels of classified information.

More detailed criteria to apply secrecy levels of TOP SECRET and SECRET are established by the Government under the provision they had previously provided an opinion of the National Security Council.

More detailed criteria to apply secrecy levels of CONFIDENTIAL and RESTRICTED are established by the Government under the proposal of the relevant minister, namely under the proposal of the head of the public authority.

Designation of Foreign Classified Information

Article 15

The document containing foreign classified information shall regain the designation of secrecy level it had been marked with in the foreign country or by the international organization.

When designating secrecy levels of the documents, for the documents intended for the co-operation with foreign countries, international organizations, namely other entities of international law, in addition to expressions referred to in Article 14 of this law the designations of secrecy levels in English may be used, such as:

1) TOP SECRET secrecy level designation for „ДРЖАВНА ТАЈНА" secrecy level;
2) SECRET secrecy level designation for „СТРОГО ПОВЕРЉИВО" secrecy level;
3) CONFIDENTIAL secrecy level designation for „ПОВЕРЉИВО" secrecy level;
4) RESTRICTED secrecy level designation for „ИНТЕРНО" secrecy level.

Time Limits of Information Secrecy

Article 16

Secrecy of information shall be terminated:

1) on the date determined in the document containing classified information;
2) if certain event determined in the document containing classified information occurs;
3) after the expiration of the term prescribed by law;
4) if secrecy is revoked;
5) if information are made available to the public.

The authorized person may amend the method determined for the termination of classified information, if there grounded reasons to do so, in accordance with the law.

The authorized person is obliged to inform the public authorities and the persons who had obtained classified information or have access to such classified information about the amendment referred to in paragraph 2 of this Article, immediately and in written form.

Termination of Secrecy on Specified Date

Article 17

If the authorized person establishes in the procedure of determination of classified information that on a certain date the reasons for which some information had been declared classified shall cease to exist, the date of secrecy termination shall be determined and marked in the document containing such information.

Termination of Secrecy by Occurrence of Certain Event

Article 18

If the authorized person establishes in the procedure of determination of classified information that on a certain date the reasons for which some information had been declared classified shall cease to exist, it shall be determined that secrecy shall be terminated when such an event begins and it shall be marked in the document containing such information.

Termination of Secrecy upon Expiration of Time Limit

Article 19

In case the termination of secrecy had not been defined in accordance with Articles 17 and 18 of this law, secrecy shall be terminated upon the expiration of the time limits prescribed by this law.

The legal time limit for the termination of secrecy of information referred to in paragraph 1 of this Article shall be determined according to the level of secrecy, as follows:

1) for TOP SECRET classified information - 30 years;
2) for SECRET classified information - 15 years;
3) for CONFIDENTIAL classified information – five years;
4) for RESTRICTED classified information – two years.

The terms referred to in paragraph 2 of this Article are counted from the date no which secrecy of information is determined.

Extension of Information Secrecy Period

Article 20

If upon the expiration of the time limit referred to in Article 19 paragraph 2 of this law there are still reasons to keep classified information, the authorized person may once extend the time limit for the termination of secrecy not longer than the period determined for certain levels of information secrecy.

In addition to the authorized person referred to in paragraph 1 of this Article, the Government may also extend the time limit for keeping classified information in the following cases:

1) if their disclosure would have irreparable severe harmful consequences for the national security and particularly important state, political, economic or military interests of the Republic of Serbia;
2) if it is prescribed by the international treaty or other international obligations of the Republic of Serbia;
3) if their disclosure would have irreparable severe harmful consequences for fundamental human and civil rights of one or more persons or if it would impair the security of one or several persons.

In the event referred to in paragraph 2 of this Article, the Government may extend the time limit for the termination of secrecy for the period determined for certain levels of information secrecy.

Revocation of Information Secrecy

Article 21

In the procedure of revocation of information secrecy it is established that information shall terminate to be classified before the expiration of the time limit referred to in Articles 17 to 20 of this law.

The decision on revocation of information secrecy shall be adopted if the facts and circumstances occur due to which information shall cease to be of interest for the Republic of Serbia.
The decision referred to in paragraph 2 of this Article shall be adopted on the grounds of periodical estimation of secrecy, proposal for revocation, namely on the grounds of the decision of the competent state authority.

Periodical Assessment of Secrecy

Article 22

The authorized person shall carry out the periodic assessment of information secrecy, on which basis the authorized person may revoke secrecy of information, as follows:
1) for TOP SECRET classified information at least once in ten years;
2) for SECRET classified information at least once in five years;
3) for CONFIDENTIAL classified information at least once in three years;
4) for RESTRICTED classified information at least once a year.
If the existence of reasons referred to in Article 21 paragraph 2 of this law is established, the authorized person shall adopt the decision on revocation of secrecy without any delay, which must have the statement of reasons.

Proposal for Revocation of Secrecy

Article 23

The user of classified information may propose to the authorized person to revoke secrecy of information.
The authorized person is obliged to consider the proposal referred to in paragraph 1 of this Article and inform the proposer accordingly.

Revocation of Secrecy in the Control Procedure

Article 24

In the control procedure, the Office of the National Council for Security and Protection of Classified Information (hereinafter referred to as the Council Office) may request the authorized person to carry out a subsequent assessment of information secrecy and adopt the decision on revocation of information secrecy on its own based on such assessment.

Revocation of Secrecy Based on the Decision of the Competent Authority

Article 25

The authorized person of the public authority shall revoke secrecy of information, namely the of the documents containing classified information and shall enable the person asking for classified information to accomplish the rights, namely the accomplishment of rights to the applicant based on the decision of the Commissioner for Information of Public Importance and Protection of Personal Data in the appeal proceedings, namely based on the decision of the competent court in the suit, pursuant to the law prescribing free access to information of public importance and the law prescribing protection of personal data.

Revocation of Secrecy in the Public Interest

Article 26

The National Assembly, the President of the Republic and the Government may revoke secrecy of certain documents, regardless of the level of secrecy, if it is in the public interest or because of the fulfilment of international obligations.

Amendment of Secrecy Level and Duration of Secrecy

Article 27

The amendment of the level of information secrecy means the designation of information with a higher, namely with a lower level of secrecy than the level of secrecy the information had until that time, before the expiration of the time limit referred to in Articles 17 to 20 of this law.
The amendment of the level and the duration of information secrecy is made by an adequate application of the provisions referred to in Articles 21 to 24 and Article 26 of this law.

Notice on Amendment of Secrecy Level and Revocation of Secrecy

Article 28

The authorized person shall immediately inform in writing the users of classified information and the persons having access to such information about the amendment of level and duration of information secrecy, as well as about the revocation of information secrecy.

Foreign Classified Information

Article 29

The amendment of level and duration of information secrecy, as well as the revocation of foreign information secrecy, is made in accordance with the contracted international treaty and established international obligations.

III. PROTECTIVE MEASURES FOR CLASSIFIED INFORMATION

Protection Criteria for Classified Information

Article 30

The public authority shall, pursuant to this law and the regulations adopted on the grounds of this law, establish the system of procedures and measures for the protection of classified information according to the following criteria:
1) level of secrecy;
2) nature of the document containing classified information;
3) assessment of threat to security of classified information.

Types of Protective Measures

Article 31

The public authority shall apply general and special protective measures in accordance with the law and the regulation adopted pursuant to law and the regulation adopted on the grounds of the law, in order to protect classified information in its possession.

General Protective Measures

Article 32

General protective measures for classified information include:
1) determination of secrecy level;
2) assessment of threat to security of classified information;
3) determination of method of use and treatment of classified information;
4) appointment of the person responsible for keeping, using, exchange and other activities concerning processing of classified information;
5) appointment of classified information operator, including also the security checkout of the operator depending on the level of information secrecy;
6) determination of special zones, buildings and remises intended for the protection of classified information and foreign classified information;
7) supervision of classified information treatment;

8) measures of physical-technical protection of classified information, including fitting in and installation of technical protective means, establishment of security zone and protection outside security zone;
9) protective measures for information-telecommunication systems;
10) measures of crypto-protection;
11) protective mode of operation for working and formation positions, within the document on internal organization and classification of working posts;
12) establishment of special educational and training programmes for the requirements of the performance of protective jobs for classified information and foreign classified information;
13) other protective measures prescribed by law.

Special Protective Measures

Article 33

With the aim to accomplish an efficient application of general protective measures for classified information referred to in Article 32 of this law, the Government document shall define special protective measures for classified information.
Certain special protective measures may be precisely defined by the document to be issued by the competent minister, namely by the head of the special organization, in compliance with the document of the Government referred to in paragraph 1 of this Article.

Obligations of the Operator

Article 34

The operator of classified information shall, in accordance with this law and within his/her authorizations, undertake protective measures for classified information and enable the users to have direct access to classified information, issue a copy of the document containing classified information, keep records of the users and take care of the exchange of classified information.

Keeping, Transfer and Submission of Classified Information

Article 35

Classified information shall be kept in such a way that access to such information shall only be allowed to the authorized users.
Classified information may be transferred and submitted outside the premises of the public authority only under the provision that prescribed security measures and procedures are respected, which provide that classified information shall only be obtained by the person having the approval for access to classified information and who has the right to obtain them.
On the occasion of the transfer and submission of classified information outside the premises of the public authorities, protective procedures and measures are determined according to the level of secrecy of such information, in accordance with the law and the regulation adopted on the grounds of the law.
The transfer and the submission of classified information by means of telecommunication-information means is carried out under the compulsory application of the prescribed measures of crypto-protection.
The application of measures of crypto-protection on the occasion of the transfer and submission of such information as referred in paragraphs 3 and 4 of this Article is carried out according to the law.

Obligation to Inform about Loss, Theft, Damage, Spoliation or Unauthorized Disclosure of Classified Information and Foreign Classified Information

Article 36

If it is learned that there has been a loss, theft, damage, spoliation or unauthorized disclosure of classified information and foreign classified information, the official, the employee, namely the person performing jobs with the public authority, shall inform the authorized person of the public authority about it and without any delay.
The person referred to in Article 35 paragraph 2 of this law, finding out that there has been a loss, theft, damage, spoliation or unauthorized disclosure of classified information and foreign classified information on the occasion of the transfer and submission of classified information outside the premises of the public authority, shall immediately inform the authorized person of the public authority who had transferred or submitted classified information and foreign classified information to him/her.
The authorized person is obliged to undertake without any delay all necessary measures to establish the circumstances that had caused a loss, theft, damage, spoliation or unauthorized disclosure of classified information and foreign classified information, make an assessment of caused damage, as well as to undertake necessary measures with the aim to eliminate the damage and prevent any new theft, damage, spoliation or unauthorized disclosure of classified information and foreign classified information.
If the case is as referred to in paragraph 3 of this Article, the authorized person shall inform the Office of the Council about the undertaken measures.

IV. ACCESS TO CLASSIFIED INFORMATION

Access to Classified Information without Approval

Article 37

The President of the National Assembly, the President of the Republic and the Prime Minister may only have the access to information and use of information and documents of any secrecy level without the issuance of approval, based on the position and with the aim to perform the jobs within their competences.

Right to Approval without Security Checkout

Article 38

The members of the Parliament, the Ombudsman, the President of the Supreme Court of Appeals, the Republic Public Prosecutor, the President and the judges of the Constitutional Court, Deputy Prime Minister, the General Secretary of the President of the Republic, the General Secretary of the Government, ministers, the official heading the administration body within the ministry, the official heading special organization, the Head of the Supreme Headquarters of the Army of Serbia, judges, public prosecutors and deputies of public prosecutors, the Republic Public Attorney, the Commissioner for Information of Public Importance and Protection of Personal Data, the Secretary of the National Security Council and the Director of the Council Office have the right to approval to access and use of classified information without the previous security checkout in order to perform the jobs within their competences.
The persons referred to in paragraph 1 of this Article are obliged to sign, before the issuance of approval, a statement confirming they will treat classified information in accordance with the law and other regulation.

Access Right to Classified Information to Members of the Competent Body of the National Assembly

Article 39

The members of the board of the National Assembly in charge of supervision and control within the defence and security sector have the right to access and review of classified information concerning the performance of supervision and control function, pursuant to the law.

Restriction of Access Right

Article 40

The access to TOP SECRET and SECRET classified information may be exceptionally restricted to the Ombudsman, the Commissioner for Access to Information of Public Importance and Protection of Personal Data and to the Director of the Council Office, pursuant to the law.
The restriction referred to in paragraph 1 of this Article relates to the information about:
1) research activity, namely the activity in progress, which is being conducted by the competent state bodies in accordance with the law, until its completion;
2) methods to provide security and intelligence information and method of application of special procedures and measures in the concrete case;
3) members of the ministry in charge of internal affairs and the security services with concealed identity, while it is necessary for the protection of vital interests of those persons, namely of the members of their families (life, health and physical integrity);
4) identities of present and former associates of the security services, while it is necessary for the protection of vital interests of those persons, namely of the members of their families (life, health and physical integrity);
5) third persons, while it is necessary, if the disclosure of information about them might be harmful for the protection of vital interests of those persons, namely of the members of their families (life, health and physical integrity).
The decision on provisional restriction of access to the information referred to in paragraph 2 of this Article shall be adopted by the body possessing classified information.
The decision referred to in paragraph 3 of this Article is to be submitted without any delay, and not later than within eight days from the date of the decision, to the board of the National Assembly in charge of supervision and control within the defence and security sector, to the Government and to the National Security Council.
If the Ombudsman, the Commissioner for Access to Information of Public Importance and Protection of Personal Data, namely the Director of the Council Office find there are no reasons for provisional restriction of access, they may request the initiation of the internal control procedure, in compliance with the provisions of this law.
The body in charge of internal control shall inform the applicant referred to in paragraph 5 of this Article, not later than 30 days from the date of the request, about the results of the performed control.
Independently of the request for the initiation of internal control procedure, the Ombudsman and the Commissioner for Information of Public Importance and Protection of Personal Data may file a request to the President of the Supreme Court of Appeals to quash such a decision within eight days from the date of the submission of the decision referred to in paragraph 3 of this Article.
The President of the Supreme Court of Appeals is obliged to decide on the request referred to in paragraph 7 of this Article within eight days from the date of the submission of the request.
When deciding on the request referred to in paragraph 7 of this Article, the President of the Supreme Court of Appeals may adopt the request and quash the decision or dismiss the

request and uphold the decision. No legal remedy is permitted against this decision of the President of the Supreme Court of Appeals.

Right to Access to RESTRICTED Classified Information

Article 41

The officials, the employees, namely the persons working at the public authorities have the access to classified information determined as RESTRICTED classified information.
The persons referred to in paragraph 1 of this Article shall sign a statement, by which they shall confirm they shall treat classified information in accordance with the law and other regulation.

Access to Foreign Classified Information

Article 42

The access to foreign classified information is made in accordance with this law, the regulations adopted on the grounds of this law, namely in accordance with the international treaty the Republic of Serbia concluded with a foreign country, and international organization or other international entity.

Natural Persons and Legal Entities as Users of Classified Information

Article 43

Natural persons and legal entities – users of classified information have the right to access to classified information necessary for the performance of jobs within the scope of their activities, which are specified in the approval for the access to classified information according to the level of secrecy (hereinafter referred to as the approval), namely in the permit.
As an exemption from paragraph 1 of this Article, in case of extreme urgency in acting, the person who had been issued the approval, namely the permit for the access to classified information of lower secrecy level, may be informed about classified information designated by the directly higher level of secrecy.
The person referred to in paragraph 2 of this Article is obliged to sign a statement confirming to treat classified information in accordance with the law and other regulation.

Statement and Approval

Article 44

Before the issuance of the approval, namely of the permit, the person who is issued the approval is obliged to sign a statement confirming to treat classified information in accordance with the law and other regulation.
If the person referred to in paragraph 1 of this Article does not sign the approval, the procedure of the issuance of the approval, namely of the permit shall be terminated.
The written statement makes an integral part of the documentation on which basis the approval, namely the permit had been issued.

Release from Duty to Keep Classified Information

Article 45

The person who had been issued the approval, namely the permit may not use the information for any other purposes except for the purposes the approval, namely the permit had been issued for.
The head of the public authority may, at the request of the competent body, release the person from the duty to keep secrecy of information by means of a separate decision, which shall also specify the measures for protection of secrecy of information, but only for the purposes and within the scope contained in the request by the competent body in accordance with the law.

At the request of the competent body, the head of the public authority may be released from the duty to keep secrecy of information by the body that had appointed, elected him/her, namely that had nominated him/her, and this body shall inform the Office of the Council accordingly.

Submission of Classified Information under Obligation to Keep Them Classified

Article 46

Classified information may be submitted to other public authority on the grounds of a written approval by the authorized person of the public authority that had determined classified information, unless some special law prescribes otherwise.
Classified information received from the public authority may not be forwarded to another user without the approval of the body that had determined classified information, unless some special law prescribes otherwise.
The persons who work with the public authority, to whom classified information referred to in paragraph 1 of this Article had been forwarded, are obliged to act in accordance with the provisions of this law, also having the obligation to comply with secrecy designations and to undertake the measures for the protection of information secrecy.

Submission of Classified Information on Contract Basis

Article 47

The authorized person may submit classified information to other natural persons and legal entities, which render services to the public authority on contract basis, if:
1) a legal entity or a natural person fulfil organizational and technical conditions to keep classified information according to this law and the regulation adopted on the grounds of this law;
2) security checkouts had been made and approvals issued for the persons performing the contracted jobs;
3) the persons referred to in item 2) of this paragraph confirm by means of a written statement that they have been informed about this law and other regulations prescribing keeping of classified information and undertake the obligation to treat classified information in accordance with such regulations;
4) the access to classified information is inevitably necessary in order to implement the jobs stipulated by the contract.
The measures for the protection of classified information resulting from paragraph 1 of this Article must be included in the contract related to the implementation of the jobs concluded between the public authority and legal entity or natural person.
The Government shall define in more details the method and the procedure how to establish the conditions referred to in paragraph 1 item 1) of this Article.

Records of Classified Information Submitted to Other Users

Article 48

The operator of the public authority shall establish and keep updated records about classified information submitted to other users outside the public authority.

V. ISSUANCE PROCEDURE OF APPROVALS AND PERMITS

Conditions for Issuance of Approval to Natural Persons

Article 49

The approval is issued by the competent body prescribed by this law, on the grounds of a written request to be made by a natural person if the person making the request:

1) is a citizen of the Republic of Serbia;
2) is of age;
3) has business capacity;
4) has not been convicted to an effective prison sentence for the criminal act prosecuted in the capacity of the office, namely for the offence specified by this law;
5) has passed an adequate security checkout.

Conditions for Issuance of Approval to Legal Entities

Article 50

The approval is issued by the competent body prescribed by this law, on the grounds of a written request to be made by a legal entity, which is submitted through the proxy, if the entity making the request:
1) has a registered seat in the territory of the Republic of Serbia;
2) performs the activities related to the interests established in Article 8 of this law;
3) has passed an adequate security checkout;
4) is not in the process of liquidation, namely bankruptcy;
5) has not been prosecuted to stop performing the activities, namely that no penalty to cease being a legal entity has been imposed against it or the measure of security prohibition to perform certain registered activities or jobs;
6) regularly pays its tax obligations, namely contributions.

Issuance of Permit to Foreign Persons

Article 51

A foreign person is issued the permit by the competent authority if:
1) the foreign person possesses an adequate security certificate issued by a foreign country the foreign person is a citizen of, namely where the foreign person has the seat or by an international organization the foreign person is a member of;
2) the obligation to provide the access to classified information results from the concluded international treaty.

Submission of Request

Article 52

A request for the issuance of the approval is submitted to the Office of the Council.
If the approval is requested by the operator or some other employee of the public authority, the request referred to in paragraph 1 of this Article shall be provided by the head of the public authority.
If the approval is requested for the legal entity and the employees of the legal entity, the request shall be submitted by the legal representative of the legal entity.
A request for the issuance of the approval to the person, who shall have the access to classified information, for the purpose of the implementation of the contracted jobs with the public authority, shall be submitted by the public authority the implementation of the contracted jobs refers to.

Contents of Request

Article 53

A request for the approval by the natural person shall contain: name and surname, residence, jobs he/she performs, reasons for the issuance of the approval, as well as the secrecy level of information the approval is requested for.
A request for the approval by the legal entity shall include: company's name, seat and activities of the legal entity, name and surname and residence of the legal representative of the

legal entity, reasons for the issuance of the approval, as well as the secrecy level of information the approval is requested for.
In addition to the information referred to in paragraph 1 or 2 of this Article, a foreign person is also to submit the security certificate referred to in Article 51 item 1) of this law.

Security Checkout

Article 54

A security checkout is made for the access and use of classified information depending on the level of secrecy, as follows:
1) basic security checkout, for RESTRICTED and CONDIFENTIAL classified information;
2) complete security checkout, for SECRET classified information;
3) special security checkout, for TOP SECRET classified information.

Body in Charge of Security Checkout

Article 55

The security checkout for the access to classified information and documents of TOP SECRET and SECRET secrecy level shall be carried out by the Security Information Agency of the Republic of Serbia.
The security checkout for the access to classified information and documents of CONFIDENTIAL and RESTRICTED secrecy level shall be carried out by the ministry in charge of internal affairs.
The security checkout for the access to classified information and documents of all secrecy levels for the persons who need the access to classified information and documents in order to perform their functions or work assignments within the ministry in charge of defence and the Army of Serbia shall be carried out by the Military Security Agency.
As an exemption from paragraph 2 of this Article, the security checkout for the access to classified information and documents of CONFIDENTIAL and RESTRICTED secrecy level for the persons who need the access to classified information and documents in order to perform their functions or work assignments at the Security Information Agency, shall be carried out by the Security Information Agency.
The security checkout for the access to SECRET classified information and documents for the persons who need the access to classified information and documents in order to perform their functions or work assignments within the ministry in charge of internal affairs, in addition to the body referred to in paragraph 1 of this Article, may be also carried out by the ministry in charge of internal affairs.
The bodies responsible for the security checkout referred to in paragraphs 1 to 5 of this Article are obliged to co-operate between each other in the procedure of the security checkout, in particular in the procedure of security checkout for the access to TOP SECRET and SECRET classified information.

Co-operation with Foreign Countries and International Organizations

Article 56

The bodies responsible for the security checkout referred to in Article 55 of this law may co-operate, in the procedure of the security checkout, with the bodies of other foreign countries, international organizations and other international subjects competent for the security checkout, in accordance with the international treaty the Republic of Serbia had concluded with the foreign country and in accordance with the regulations prescribing the protection of personal data in the Republic of Serbia.

Purpose of Security Checkout

Article 57

The security checkout of the applicant shall provide an assessment of security risk, especially of the risk from the access and use of classified information.
Within the security checkout the competent body shall assess the data in the filled questionnaire from the security view point.
The competent body, in respect of the data stated in the security questionnaire, shall collect personal and other data from the person such data refer to, from other public authorities, organizations and persons, from the registry, records, data bases and data collections that are kept pursuant to the law.

Security Questionnaire

Article 58

In order to make the security checkout, the Office of the Council shall submit a security questionnaire to the applicant.
The applicant shall fill in the basic security questionnaire, and if the approval is requested for classified information of TOP SECRET and SECRET secrecy levels, the applicant shall also fill in the special security questionnaire.
The questionnaire filled in and signed by the applicant is simultaneously a written approval to make the security checkout and is designated as RESTRICTED classified information.

Basic Security Questionnaire for Natural Persons

Article 59

The following information about the applicant are to be filled in the basic security questionnaire:
1) name and surname, as well as former names and surnames;
2) personal identification number;
3) date and place of birth;
4) citizenship, former citizenships and dual citizenships;
5) permanent residence and temporary residence, as well as previous residences;
6) marital status and family status;
7) information about the persons living in the common household with the person the security questionnaire refers to (their names and surnames, together with former names and surnames, their dates of birth, as well as their relationship with the person being checked up);
8) name and surname, date of birth and address of residence of the relative up to the second line of ascent in the straight and up to the first line of ascent in the side line, adopted persons, custodians, step-fathers, step-mothers, namely foster parents;
9) qualifications and profession;
10) information about former employments;
11) information related to military service;
12) information about criminal and tortuous sanctions and criminal and tortuous proceedings in progress;
13) medical data concerning addiction (alcohol, narcotics, etc.), namely mental illness;
14) contacts with foreign security services and intelligence services;
15) disciplinary procedures and inflicted disciplinary measures;
16) information about membership or participation in the activities of organizations whose activities and objectives are prohibited;
17) information about responsibility for violation of regulations related to secrecy of information;

18) information about property rights or other real estate right, information about property right over other assets registered in the public registry, as well as information about annual tax on total income of citizens for previous year;

19) previous security checkouts.

Basic Security Questionnaire for Legal Entities

Article 60

The following information about the applicant are to be filled in the basic security questionnaire for legal entities:

1) name and seat of company, as well as the former names and seats of companies;
2) registration number of legal entity and tax identification number;
3) name and surname of the legal representative;
4) date and place of establishment;
5) information about organizational units, branches, dependent companies and other forms of relations;
6) origin of initial capital including amendments within the last three years;
7) number of employees;
8) number of employees the approval is requested for and type of jobs they perform;
9) information about convictions for criminal acts, business offence and offence of legal entity and responsible persons with the legal entity, as well as information about proceedings for criminal acts, business offence or offence against legal entity that are in progress;
10) information about contacts with foreign security services and intelligence services;
11) information about participation in the activities of organizations whose activities and objectives are prohibited;
12) information about responsibility for violation of regulations related to secrecy of information;
13) information about previous security checkouts;
14) information about property rights or other real estate right, information about property right over other assets registered in the public registry, as well as information about the annual financial report for the previous year in accordance with the law prescribing accounting and auditing.

Together with the filled in questionnaire referred to in paragraph 1 of this Article, the legal representative of the legal entity shall also submit a filled in basic security questionnaire for natural person.

Special Security Questionnaire

Article 61

As for the security checkout established in Article 54 items 2) and 3) of this law, in addition to the basic security questionnaire, the special security questionnaire is also to be filled in.

The following information are to be entered in the special security questionnaire:

1) information about employment with foreign armies and paramilitary formations;
2) other information and facts, in addition to the information stated in Articles 59 and 60, which make natural persons, namely legal entities susceptible to effects and pressures representing risks to security;
3) information about debts resulting from financial liabilities or undertaken guarantees.

Subject of Security Checkout and Questionnaire Form

Article 62

The information from the questionnaire referred to in Articles 59 to 61 of this law present the subject of an adequate security checkout.

The forms of the questionnaire referred to in paragraph 1 of this Article are prescribed by the Government under the proposal of the Office of Council.

Special Security Checkout

Article 63

The special security checkout is made when the issuance of the approval, namely of the permit is requested for TOP SECRET classified information.
The special security checkout also includes, in addition to the checkout of the facts within the complete security checkout, the checkout of facts, circumstances and events from the private life of the applicant, at least within the last ten years from the date of the submission of request for the issuance of the approval, which, if they exist, would be the grounds of doubt about his/her confidentiality and reliability, especially if his/her activities are contrary to the interests of the Republic of Serbia, or if he/she is related with foreign persons who might impair the security and the international interests of the Republic of Serbia.

Time Limits for Completion of Security Checkout

Article 64

The competent body is obliged to make the security checkout after the date of the receipt of the filled in questionnaire within the following time limits:
1) up to 30 days for the complete security checkout;
2) up to 60 days for the complete security checkout;
3) up to 90 days for the special security checkout.
Exceptionally, in case of justified reasons, the time limits referred to in paragraph 1 items 2) and 3) of this Article may be extended for the period established in these items at maximum.
If there is a case as referred to in paragraph 2 of this Article, the competent body is obliged to inform the head of the public authority about the extension of the time limit, which had submitted a request for the security checkout as well as the Office of the Council.
If the security checkout is not made within the time limits specified in paragraphs 1 and 2 of this Article, it shall be deemed that there is no security risk for the access to classified information of the applicant.

Provisional Approval

Article 65

In order to perform urgent jobs and assignments of the public authority, and with the aim to prevent or eliminate damage, the Director of the Office of the Council may exceptionally and before the completion of the security checkout, issue the approval for the access to certain classified information, if the Director estimates, after the review of the submitted security questionnaire, that there are no doubts in respect of security.
The person referred to in paragraph 1 of this Article is obliged to confirm by means of written statement that classified information entrusted to him/her shall be treated in accordance with this law and other regulations governing keeping and treatment of classified information.
The provisional approval referred to in paragraph 1 of this Article shall be valid until the date of the completion of the procedure for the issuance of the approval.

Submission of Report on Results of Security Checkout

Article 66

The bodies competent for the security checkout referred to in Article 55 of this law, shall submit to the Office of the Council the report on the results of the security checkout, namely of the special security checkout, also including the filled in security questionnaire with a recommendation to issue or refuse the approval.

In the report referred to in paragraph 1 of this Article, no sources of the security checkout shall be mentioned.
The report and the recommendation referred to in paragraph 1 of this Article shall be determined as CONFIDENTIAL classified information.

Decision and Additional Checkout

Article 67

The Office of the Council shall decide on the issuance of the approval by means of a decision, within 15 days from the date of the submission of the report containing the recommendation referred to in Article 66 paragraph 1 of this law, namely from the expiration of the time limit to make the security checkout referred to in Article 64 of this law.
If the report is incomplete or if it had been submitted without the recommendation, the Office of the Council shall adopt the decision on the grounds of the submitted report.
In exceptional cases, if it cannot be determined from the report on the results of the security checkout and the recommendation for the issuance of the approval whether the conditions prescribed by law for the issuance of the approval to natural persons or legal entities have been fulfilled or not, or whether some substantial amendments of the checked out data have taken place after the security checkout, which might be of influence to the issuance of the approval, the Office of the Council shall request from the competent body referred to in Article 55 of this law to carry out an additional checkout, namely a supplement of the report and the preparation of new recommendation, not later than within a subsequent term of 30 days.

Exemptions

Article 68

For the persons who need access to classified information in order to perform their functions or work assignments at the security services of the Republic of Serbia, as an exception from Article 67 of this law, the decision on the issuance of the approval for the access to classified information at the disposal of the security service, shall be adopted by the head of the service referred to in Article 55 paragraphs 3 and 4 of this law.

Submission of Decision

Article 69

The Office of the Council shall submit the decision to the head of the public authority who had requested the issuance of the approval and to the person the approval had been requested for.

Dismissal of Request

Article 70

By means of a decision the Office of the Council shall dismiss the request for the issuance of the approval if, based on the report of the security, namely of the additional security checkout, it is established that:
1) the applicant had stated false and incomplete information in the basic, namely in the special security questionnaire;
2) the applicant does not meet the requirements for the issuance of the approval, namely of the permit referred to in Articles 49 to 51 of this law;
3) the applicant had not provided the conditions to undertake the proper measures to protect classified information;
4) there is security risk for the access and use of classified information of the applicant.
The statement of reasons of the decision on the dismissal to issue the approval shall not contain the information considered classified within the meaning of this law and nor sources of the security checkout shall be stated.

Adequate Application

Article 71

The provisions of the law prescribing the general administrative procedure shall be applied to the procedure of issuance of the approval, namely of the permit, unless this law prescribes otherwise.

Administrative Dispute

Article 72

The decision of the Office of the Council shall be final.
The applicant whose request had been dismissed or who had not been granted the approval within the time limit prescribed in Article 67 of this law, may initiate an administrative dispute against the Office of the Council.

Contents, Form and Submission of Approval

Article 73

The contents, the form and the method of submission of the approval shall be prescribed by the Government under the proposal of the Office of the Council.
The Office of the Council shall submit the approval and inform the user about the prescribed conditions how to treat classified information, as well as about legal and other consequences of their unauthorized use.
On the occasion of the receipt of the approval, the user shall sign the approval, as well as the statement that he/she had been informed about the provisions of the law and other regulations prescribing the protection of classified information and that he/she shall use classified information in accordance with the law and other regulation.

Expiration of Approval Validity

Article 74

The approval shall cease to be valid:
1) upon the expiration of the period it had been issued for;
2) upon the termination of the function of the person referred to in Article 38 of this law;
3) upon the termination of duties and jobs within the scope of activities of the person referred to in Article 41 of this law;
4) on the grounds of the decision adopted by the Office of the Council in the checkout procedure of the issued approval;
5) if the natural person dies or the legal entity ceases to exist, which had been granted the approval.

Expiration of Approval Validity after Specified Date

Article 75

The approval issued for TOP SECRET classified information and the document shall be valid for three years.
The approval issued for SECRET classified information and the document shall be valid for five years.
The approval issued for CONFIDENTIAL classified information shall be valid for ten years.
The approval issued for RESTRICTED classified information and the document shall be valid for 15 years.

Extension of Approval Validity

Article 76

The Office of the Council shall inform the holder of the approval in writing about the possibility to submit a request for the extension of validity of the approval, not later than six months before the expiration of validity of the approval.
Together with the request for the extension of validity referred to in paragraph 1 of this Article, the applicant shall inform the Office of the Council about all amendments of information contained in the previously submitted security questionnaire with evidence, and the competent body referred to in Article 55 of this law shall make the security checkout again.
The provisions contained in Articles 49 to 64 and Article 67 of this law shall be applied to a new security checkout referred to in paragraph 2 of this Article, unless the international treaty prescribes otherwise.

Provisional Prohibition of Access Right

Article 77

If any disciplinary procedure had been initiated against the person to whom the approval was granted, for a severe violation of the capacity of the office, a severe violation of military discipline, namely for a severe violation of work assignments and duties, criminal proceedings because of grounded doubt that such the person had committed a criminal act prosecuted in the capacity of the office, namely tortuous proceedings for an offence prescribed by this law, the head of the public authority may temporarily prohibit, by means of a decision, the access to classified information to such a person until the proceedings are finally closed.

Checkout of Approval

Article 78

If it is found out that the person having been granted the approval, does not use classified information or does not keep them in accordance with this law and other regulations, namely that such a person does not meet the requirements for the issuance of the approval any longer, the Office of the Council shall adopt the decision on the termination of validity of the approval before the expiration of its validity, namely it shall adopt the decision restricting the right to access to classified information of certain secrecy level.
The statement of reasons referred to in paragraph 1 of this Article shall not contain any information considered classified within the meaning of this law.
The decision of the Office of the Council referred to in paragraph 1 of this Article shall be final and the administrative proceedings may be initiated against it.

Issuance of Permit to Foreign Persons

Article 79

The Office of the Council shall issue the permit to a foreign person, in accordance with the concluded international treaty.
Upon the receipt of the request, the Office of the Council shall check, by means of the international exchange, whether the applicant had been issued the security certificate by the state he/she is a citizen of or where it has the seat in, namely by the international organization he/she is a member of.
The permit is only issued for the access to the information and the documents established in the concluded international treaty, which the Republic of Serbia concluded with a foreign country, an international organization or other international subject.
The provisions of this law concerning the issuance of approval shall be accordingly applied to the issuance of the permit to a foreign person.

Official Records and Other Information Related to Approval and Permit

Article 80

The Office of the Council shall keep the uniform central records of issued approvals and permits, decisions on issuance of approvals and permits, decisions on dismissal of issuance of approvals and permits, decisions on extension of validity of approvals and permits and decisions on restriction or termination of validity of approvals and permits, as well as of the signed statements by the persons who had been granted the approval, namely the permit.
The Office of the Council shall keep the requests for the issuance of approvals, namely permits, security questionnaires and reports on security checkouts with the recommendation.

Records of Security Checkouts

Article 81

The body in charge of the security checkout referred to in 55 of this law, shall keep records of the security checkouts and keep the documents about the security checkouts together with a copy of the report and the recommendation.
The information contained in the security checkout may only be used for the purposes they had been collected for.

Application of Regulations on Protection of Personal Data

Article 82

Any person has the right to review of the data contained in his/her security checkout, which had been collected pursuant to this law, as well as other rights on the grounds of the review in accordance with the law prescribing the protection of personal data, except for the review of the information that would disclose the methods and procedures used during the collection of information, and except for the information that would identify the sources of information contained in the security checkout.

Records of Public Authorities

Article 83

The public authority shall keep records of the decisions on the approval for the persons who perform certain functions within the public authority or who are employed with it, namely for the persons who perform duties with it.
The decision on the issued approval for the persons referred to in paragraph 1 of this Article shall be kept in the special part of the human resources file of the person, and the data contained in the decision may be used in relation with the implementation of the provisions of this law, namely the regulation adopted on the grounds of this law.

More Detailed Regulation on Contents, Form and Method of Keeping Records

Article 84

The contents, the form and the method of keeping records as well as the period of records keeping referred to in Articles 80, 81 and 83 of this law shall be prescribed by the Government under the proposal of the Office of the Council.

VI. MONITORING

1. INTERNAL CONTROL

Article 85

The head of the public authority is responsible for the internal control of the enforcement of this law and the regulation adopted on the grounds of this law.

At the ministry in charge of internal affairs, at the ministry in charge of defence affairs and at the Security Information Agency, and, if necessary, at other public authorities, there shall be a special work post for internal control and other expert jobs concerning classification and protection of classified information, or the existing organizational unit within the framework of the ministries or the agency is separately engaged to perform these assignments and jobs.

Objective of Internal Control

Article 86

The internal control shall provide regular monitoring and assessment of certain activities, as well as the activities of the public authority as a whole, concerning the enforcement of this law and the regulations and the measures adopted on the grounds of this law.
The head of the public authority, either directly or through an authorized person, shall perform the internal control by direct review, adequate checkouts and by examination of the submitted reports.

2. THE OFFICE OF THE COUNCIL

The Status of the Council Office

Article 87

The Office of the Council is an agency of the Government having the properties of a legal entity, having the competence to implement certain jobs of enforcement and control of enforcement of this law and supervision over the enforcement of this law.

Competence of the Council Office

Article 88

In accordance with this law, the Office of the Council shall:
1) monitor the conditions and provide the application of standards and regulations within the field of protection of classified information;
2) take care of the implementation of the accepted international obligations and concluded international treaties between the Republic of Serbia and other countries, namely between the international bodies and organizations in the field of protection of classified information and co-operate with the relevant bodies from foreign countries and of international organizations;
3) establish and keep the Central Registry of Foreign Classified Information;
4) prepare the regulations necessary for the enforcement of this law;
5) render opinions about the drafts of regulations in the field of protection of classified information;
6) propose to the Government the contents, the form and the method how to keep records of classified information;
7) propose to the Government the form of security questionnaire;
8) propose to the Government the form of recommendation, approval and permit;
9) keep records of the issued approvals, namely of the permits, as well as the records of dismissals to issue the approvals, namely the permits;
10) order the measures for the improvement of protection of classified information;
11) arrange the training of the users of classified information in accordance with the relevant standards and regulations;
12) propose to the Government the plan of protection for classified information for extraordinary and urgent cases;
13) control the application of the criteria to designate the levels of secrecy and carry out other control jobs in accordance with the provisions of this law;
14) revoke secrecy of information in accordance with the provisions of this law;

15) carry out the jobs related to the protection of classified information after the public authorities having no legal successor cease to exist;

16) file criminal charges, requests to initiate tortuous proceedings and propose the initiation of other proceedings because of violations of the provisions of the law, pursuant to the law;

17) co-operate with the public authorities in the enforcement of this law;

18) perform other jobs prescribed by this law and the regulation adopted on the grounds of this law.

The Director of the Office of the Council shall submit to the Government and the board of the National Assembly in charge of monitoring and control with the sector of defence and security, the annual report on the activities concerning the activities of enforcement and control of enforcement of this law.

Taking Over Classified Information

Article 89

The Office of the Council shall take over classified information of the public authorities that ceased to exist, having no legal successor, namely it shall oblige another public authority to keep and use such information.

Director of the Council Office

Article 90

The Government shall appoint and remove from the duty the Director of the Office of the Council, after the provision of the opinion from the National Security Council.

The Director of the Office of the Council shall be appointed for the period of five years.

The same person may be appointed the Director of the Office of the Council only twice at maximum.

The person meeting the general requirements of employment with the state authorities shall be appointed the Director of the Office of the Council, who has a university degree and at least ten years of experience doing the jobs in the field of security.

The Director of the Office of the Council cannot be a member of any political party.

The Director of the Office of the Council shall be responsible to the Government and the Prime Minister.

The Director of the Office of the Council shall be a civil servant having a position.

Termination of Duty

Article 91

The job at the position of the Director of the Office of Council shall be terminated for the reasons established by law prescribing the rights and obligations of civil servants.

The Director of the Office of the Council shall be released from duty for the reasons established by law prescribing the rights and obligations of civil servants, and if he/she becomes a member of some political party.

Deputy Director of the Council Office

Article 92

The Office of the Council has the Deputy Director, who is appointed by the Government, as proposed by the Director of the Office of the Council.

The Deputy Director of the Office of the Council shall be appointed for the period of five years.

The person meeting the general requirements of employment with the state authorities shall be appointed the Deputy Director of the Office of the Council, who has a university degree and at

least nine years of experience doing the jobs in the field of protection of classified information.
The Deputy Director cannot be a member of any political party.
The Deputy Director of the Office of the Council shall be a civil servant having a position.
The Deputy Director shall perform the functions of the Director of the Office of the Council in case of absence, death, expiration of mandate, removal from the office and temporary or permanent inability of the Director of the Office of the Council to do his/her job.
The job at the position of the Deputy Director of the Office of Council shall be terminated for the reasons established by law prescribing the rights and obligations of civil servants.
The Deputy Director of the Office of the Council shall be released from duty for the reasons established by law prescribing the rights and obligations of civil servants, and if he/she becomes a member of some political party.

Document on Internal Organization and Classification of Work Posts and Salary Increase

Article 93

The Director of the Office of the Council shall adopt the document on internal organization and classification of work posts, to be approved by the Government, after the provision of the opinion from the National Security Council.
The person doing the jobs of protection of classified information may be employed at the Office of the Council if he/she had gone through the special security checkout.
The regulations concerning the labour relations of the civil servants and the employees shall be applied to the labour relations of the Director of the Office of the Council, the Deputy Director of the Office of the Council and the employees of the Office of the Council doing the jobs of the protection of classified information.
Because of the special working conditions, complexity and nature of the jobs, the Director of the Office of the Council, the Deputy Director of the Office of the Council and the employees of the Office of the Council doing the jobs of the protection of classified information, may get salary increase of up to 20% in relation to the salary of the civil servants and the employees whose work posts are classified in the same group, namely of those who have the same positions as well as the work posts of civil servants and employees doing the jobs of the protection of classified information, pursuant to the document of the Government.

Obligations of the Council Office Related to Foreign Classified Information

Article 94

The exchange of classified information with foreign countries and international organizations is carried out through the Office of the Council, unless the separate law or the concluded international treaty prescribes otherwise.

Central Registry of Foreign Classified Information

Article 95

The Office of the Council shall establish, manage and provide the Central Registry of Foreign Classified Information and Documents.
The public authority, which had received some foreign classified information and document in accordance with the separate law or the contracted international treaty the Republic of Serbia had concluded with a foreign country, an international organization or other international subject, shall establish, manage and provide the separate registry of foreign classified information.
The report containing numerical indicators about the exchange of classified information with a foreign country, an international organization, shall be submitted by the public authority to the Office of the Council at least once a year.

Issuance and Receipt of Notices

Article 96

The Office of the Council shall inform the foreign country, namely the international organization about the security of foreign classified information obtained within the international exchange.
The Office of the Council shall receive notices from the foreign country, namely from the international organization about the security of classified information that the Republic of Serbia submitted in the international exchange.

Exchange of Information without the Concluded International Treaty

Article 97

Under extremely adverse political, economic or defence-security circumstances for the Republic of Serbia and if it is necessary for the protection of interests referred to in Article 8 paragraph 2 of this law, at the request of the public authority, the Office of the Council shall exchange classified information with a foreign country, an international organization even without the previously concluded treaty.

VII. PENALTY PROVISIONS

Criminal Act

Article 98

Anyone who shall declare, submit or make available without authorization to an unknown person the information or the documents entrusted to him/her or the information and the documents obtained in another way or who shall collect the information or the documents, which present classified information of RESTRICTED secrecy level or CONFIDENTIAL secrecy level, as prescribed by this law, shall be sanctioned to a prison sentence from three months to three years.
If the act referred to in paragraph 1 of this Article has been committed in relation to SECRET classified information, pursuant to this law, the perpetrator shall be sanctioned to a prison sentence from six months to five years.
If the act referred to in paragraph 1 of this Article has been committed in relation to TOP SECRET classified information, pursuant to this law, the perpetrator shall be sanctioned to a prison sentence from one to ten years.
If the act referred to in paragraphs 1 to 3 of this Article has been committed from expedience or in order to publish or use classified information abroad or if it has been committed during war or state of emergency, the perpetrator shall be sanctioned for the act referred to in paragraph 1 of this Article to a prison sentence from six months to five years, for the act referred to in paragraph 2 of this Article to a prison sentence from one to eight years and for the act referred to in paragraph 3 of this Article to a prison sentence from five to fifteen years.
If the act referred to in paragraphs 1 to 3 of this Article has been committed from negligence, the perpetrator shall be sanctioned for the act referred to in paragraph 1 of this Article to a prison sentence of up to two years, for the act referred to in paragraph 2 of this Article to a prison sentence from three months to three years and for the act referred to in paragraph 3 of this Article to a prison sentence from six months to five years.

Tortuous Liability of the Responsible with the Public Authority

Article 99

The responsible person with the public authority shall be fined in the amount from 5,000 to 50,000 dinars if:

1) he/she shall determine the data and the document as classified obviously not referring to the protected interests (Article 8 paragraph 2);
2) he/she shall transfer the authorization for the determination of classified information to third persons (Article 9 paragraph 3);
3) he/she shall determine information contained in the document to have an inadequate level of secrecy (Article 11 paragraph 2);
4) he/she shall adopt the decision on the determination of classified information without the statement of reasons (Article 11 paragraph 4);
5) he/she shall not revoke the secrecy of information after the date or the event of expiration of secrecy of information (Articles 17 and 18);
6) he/she shall not revoke the secrecy of information after the expiration of the legal time limit for expiration of secrecy of information (Article 19);
7) he/she shall not conduct periodical assessment of secrecy of information (Article 22);
8) he/she shall not revoke the secrecy of information on the grounds of the decision of the Commissioner for Information of Public Importance and Protection of Personal Data or the decision of the competent court (Article 25);
9) he/she shall change the level of secrecy of the document contrary to the provisions of Article 27 of this law;
10) he/she shall fail to inform the public authorities about the change of secrecy level and revocation of secrecy (Article 28);
11) he/she shall not prescribe, organize and monitor the general and the special measures for the protection of classified information, which are suitable for the level of their secrecy (Articles 32 and 33);
12) he/she shall not submit or shall not submit within the specified time limit, the decision on provisional restriction of access to information (Article 40 paragraph 4);
13) he/she shall not inform or shall not inform within the specified time limit, the applicant about the results of internal control (Article 40 paragraph 6).
14) he/she shall not submit for signature to the person provided with the approval for the access to classified information, the statement about being informed on the regulations prescribing the protection of classified information (Article 43 paragraph 3);
15) he/she shall submit classified information to legal entities and natural persons contrary to the provision of Article 47 of this law;
16) he/she shall not keep records of the decisions on the approval for access to classified information (Article 83 paragraph 1);
17) he/she shall not keep the decision on access to classified information in a separate part of the human resources file (Article 83 paragraph 2);
18) he/she shall not organize internal control of the protection of classified information (Article 85 paragraph 1);
19) he/she shall not undertake measures to establish, manage and provide the special registry of foreign classified information (Article 95 paragraph 2);

Tortuous Liability of Classified Information Operator

Article 100

The operator of classified information shall be fined for an offence in the amount from 5,000 to 50,000 dinars, who shall not undertake measures for the protection of classified information (Article 34).

VIII. TRANSITIONAL AND FINAL PROVISIONS

Article 101

The Office of the National Security Council, established in accordance with Article 8 of the Law on Organization of Security Services of the Republic of Serbia (the Official Bulletin of

RS, no. 116/07), shall continue to perform its activities under the name of the Office of the National Council for Security and Protection of Classified Information on the date this law enters into force.
The Director of the Office of the National Security Council, who had been appointed pursuant to paragraph 1 of this Article of the law, shall continue to perform the function of the Director of the Office of the National Security Council and Protection of Classified Information until the expiration of the period he/she had been appointed for.

Appointment of Deputy Director

Article 102

The Government shall appoint the Deputy Director of the Office of the Council within three months from the date of this law entering into force.

Adoption of the Document on Internal Organization and Classification of Work Posts and Transfer of Employees

Article 103

The document on internal organization and classification of work posts within the Office of the Council shall be adopted within 60 days from the date of this law entering into force.
The Office of the Council shall take over the required number of employees from other bodies of the public authority performing jobs in the field of classified information within 90 days from the date of the adoption of the document referred to in paragraph 1 of this Article.

Adoption of By-laws

Article 104

By-laws prescribed by this law, which are adopted by the Government, shall be adopted within the period of six months from the date of this law entering into force.
By-laws prescribed by this law, which are adopted by other public authorities, shall be adopted within the period of one year from the date of this law entering into force.
Before the by-laws referred to in paragraphs 1 and 2 of this Article are adopted, the provisions of the valid by-laws not contrary to the provisions of this law shall be applied.

Re-examination of Existing Secrecy Designations

Article 105

From the date of this law entering into force, the information and the documents determined to be classified in respect of secrecy level according to the previously adopted regulations, shall regain the type and the level of secrecy determined according to the previous regulations.
The heads of the public authorities shall re-examine the secrecy levels of the information and the documents referred to in paragraph 1 of this Article within the period of two years from the date of this law entering into force, in accordance with the provisions of this law.

Co-ordination of By-laws and Issuance of Approval to Employees of Public Authorities

Article 106

The public authorities are obliged to co-ordinate, within the period of one year from the date of this law entering into force, their organization with the provisions of this law.
The public authorities are obliged to organize that, within the period of two years from the date of this law entering into force, all employees, who must have access to classified information because of their work assignments or functions, are provided with the approval for the access to classified information, pursuant to this law.

Co-ordination of International Treaties

Article 107

Within the period of two years from the date of this law entering into force, the competent authorities of the Republic of Serbia shall re-examine the provisions of the existing international treaties, which the Republic of Serbia had concluded in the field of the protection of classified information and, if necessary, they shall initiate the procedure for the amendment of the international treaties.

Application of Valid Laws in the Part Relating to Determination and Protection of Classified Information

Article 108

The provisions of the existing laws prescribing the activities of the public authorities, in the part concerning the determination and protection of classified information and foreign classified information, which are not contrary to the provisions of this law, shall be applied until the date of the commencement of enforcement of this law.

Expiration of Validity of Laws and Other Regulations

Article 109

On the date of the commencement of enforcement of this law, the validity of the following shall be terminated:

1) Article 123 of the Law on Defence (the Official Bulletin of RS, no. 116/07);

2) provisions of Chapter VI – Security and Protective Measures pursuant to Articles 67 to 86 of the Law on Defence (the Official Bulletin of RS, nos. 43/94, 11/95, 28/96, 44/99 and 3/02 and (the Official Bulletin of RS, no. 116/07 – other law);

3) Article 45 paragraph 2 of the Law on Personal Data Protection (the Official Bulletin of RS, no. 97/08).

Law Entering into Force

Article 110

This law shall enter into force eight days after its publication in the Official Gazette of the Republic of Serbia and it shall be enforced as from 1 January 2010.

STATEMENT-OF-REASONS

I. CONSTITUTIONAL GROUNDS

The constitutional grounds for the adoption of the Law on Secrecy of Information is contained in Article 97 of the Constitution of the Republic of Serbia, which prescribes that the Republic of Serbia establishes and provides, *inter alia*, the security of the Republic of Serbia and the relations with other countries and international organizations (item 1), the proceedings before the state authorities (item 2) and defence and security of the Republic of Serbia (item 4).

II. REASONS TO ADOPT THE LAW

The Republic of Serbia is one of the rare countries in Europe, where the issue of the legal mode of classified information has not been defined by one law, in a comprehensive and precise manner. The present circumstances, where this issue has been defined in more than 400 mainly by-laws, is not sustainable, from both the view point of protection of the national security and from the aspect of legal certainty and undisturbed co-operation with other states and international organizations.

The most precise definition of classified information in the existing regulations may be found in the law prescribing the criminal matter, namely in the Criminal Code (Article 316 – Disclosure of Top Secret, Article 369 – Disclosure of Business Secret and Article 415 – Disclosure of Military Secret). An additional problem is the fact that the comparative legal solutions do not support the classifications of secrets to state, official or military and find it a relic from the past. The modern legislations of other countries prescribe that the classification of secrets is not made in relation to the state bodies they had resulted from but in relation to the contents and the procedure for classification of secrecy and data keeping.

The valid standard solutions in the Republic of Serbia do not provide a sufficient level of transparency and they are not the guarantee of proper conduct of the courts, the Ombudsman, the Commissioner for Information of Public Importance and Protection of Personal Data and other state bodies.

The most important objective of the proposed law is that one single law shall prescribe the criteria on which basis foreign and domestic information of interest for the Republic of Serbia shall be determined as classified information, to define the authorized persons to determine secrecy of information, to prescribe in a uniform way the regulations determining secrecy levels, the method how to determine secrecy levels, as well as to precisely establish the time limits and the conditions of termination of secrecy of information. In addition, it is necessary to appoint the body to be competent at the national level to enforce and control the enforcement of the law. The most opportune solution is that this body is the Office of the National Security Council, which is also in accordance with the comparative legal experience and requirements that these jobs are performed by the state body, which is most frequently an agency of the Government. Also, the law precisely establishes the conditions to issue approvals, namely permits for access to classified information.

When drafting the law, the comparative legal analyses were used, whereas the solutions from the states close to Serbia in respect of the level of social, security and democratic development were used.

III. EXPLANATION OF BASIC LEGAL INSTITUTES AND INDIVIDUAL SOLUTIONS

Article 1 of the law specifies the subject of the law, namely it prescribes that this law shall prescribe a uniform system of classification and protection of classified information, which are of interest for the national and public security, defence, internal and foreign affairs of the Republic of Serbia, access to classified information and termination of their secrecy, competence of authorities and monitoring of enforcement of this law, as well as the responsibility for non-fulfilment of obligations ad other issues of importance for secrecy of information.

Article 2 of the law specifies the explanation of expressions used in the law.
Articles 3 to 7 of the law define information that are not classified, the right to access to classified information, purpose of collection, keeping and use of classified information. Also, it is defined that the protection of business and other secret shall be prescribed by separate laws.
Articles 8 to 29 of the law prescribe the determination of classified information, types of information that can be classified, persons authorized to determine secrecy of information, general provisions about the procedure of classification of information secrecy, method of designation, levels of secrecy and contents of classified information, duration of secrecy, methods of termination of information secrecy, revocation of information secrecy and amendment of secrecy level and duration.
Article 14 of the law defines that classified information may have four levels of secrecy: TOP SECRET, SECRET, CONFIDENTIAL and RESTRICTED. Detailed criteria to classify TOP SECRET and SECRET levels of secrecy are established by the Government, after the previous provision of the opinion of the National Security Council, and CONFIDENTIAL and RETRICTED levels of secrecy are classified by the Government under the proposal of the competent ministry, namely under the proposal of the head of the public authority.
Article 15 of the law prescribes the determination of foreign classified information, and the designation of secrecy levels in English are co-ordinated with the designations of levels of secrecy prescribed in Article 14 of this law.
Article 19 of the law precisely defines the legal time limits after which classified information are terminated to be classified. For TOP SECRET secrecy level the time limit is 30 years, for SECRET secrecy level the time limit is 15 years, for CONFIDENTIAL secrecy level the time limit is five years and for RESTRICTED the time limit is two years, counting from the date of the classification of information.
Articles 30 to 36 of the law prescribe protective measures for classified information, namely the criteria, types of protective measures, which may be general and special, obligations of the operator of such classified information to apply protective measures, as well as the duty of notices in case of a loss, theft, damage, spoliation or unauthorized disclosure of classified information and foreign classified information**.**
Article 37 of the law prescribes that only the President of the National Assembly, the President of the Republic and the Prime Minister may have the access to information and use of information and documents of any secrecy level without the issuance of approval, based on the position and with the aim to perform the jobs within their competences.

Article 38 of the law prescribes that the members of the Parliament, the Ombudsman, the President of the Supreme Court of Appeals, the Republic Public Prosecutor, the President and the judges of the Constitutional Court, the Prime Minister the Deputy Prime Minister, the General Secretary of the President of the Republic, the General Secretary of the Government, ministers, the official heading the administration body within the ministry, the official heading special organization, the Head of the Supreme Headquarters of the Army of Serbia, judges, public prosecutors and deputies of public prosecutors, the Republic Public Attorney, the Commissioner for Information of Public Importance and Protection of Personal Data, the Secretary of the National Security Council and the Director of the Council Office have the right to approval to access and use of classified information without the previous security checkout in order to perform the jobs within their competences.
The above mentioned persons are obliged to sign, before the issuance of approval, a statement confirming they will treat classified information in accordance with the law and other regulation.
Article 39 of the law prescribes that the members of the board of the National Assembly in charge of monitoring and control within the defence and security sector have the right to access and review of classified information concerning the performance of monitoring and control function, pursuant to the law.

Article 40 of the law prescribes special restrictions of the right to access to classified information of TOP SECRET and SECRET levels. It is prescribed that exceptionally the Ombudsman, the Commissioner for Access to Information of Public Importance and Protection of Personal Data and to the Director of the Council Office may have restricted access to classified information with the highest secrecy level for the precisely prescribed reasons, such as: research activities or actions that are in progress, the methods of collection of security or intelligence information, as well as the information about the officials with concealed identity and protected witnesses. The proposed solution shall be used to implement the democratic principle that no one shall have the access to all classified information, neither the representatives of the state authorities nor the representatives of „control" bodies. In order to prevent the abuse of restriction of the rights, the Commissioner for Access to Information of Public Importance and Protection of Personal Data and the Ombudsman have the right to court protection, in the way that they may file a request to the President of the Supreme Court of Appeals to quash the decision on the restriction of the right to classified information. In addition, the mechanism of internal control has also been foreseen, and the obligation prescribed that the decision restricting the right to the access is to be submitted to the competent board of the National Assembly, the Government and the National Security Council.

Articles 43 to 48 of the law prescribe the conditions under which natural persons and legal entities may be the users of classified information. Also, the procedure of the issuance of the statement and the approval for the access to classified information to users is specified, as well as the release from the duty to keep secrecy, submit classified information under the obligation to keep secrecy, submit classified information on contract basis and keep records of classified information to be submitted to other users.

Articles 49 to 84 of the law define the procedure of issuance of approval or permit for the access to classified information.

Article 49 of the law prescribes the conditions for the issuance of approval to natural persons. Natural persons may file a written request for the issuance of approval for the access to certain classified information if he/she is a citizen of the Republic of Serbia, of age and has business capacity, if he/she had not been convicted to effective prison sentence for the criminal act prosecuted in the capacity of the office, namely for the offence prescribed in this law and if he/she had gone through an adequate security checkout.

Articles 50 and 51 of the law prescribe the conditions for the issuance of the approval to legal entity and foreign person.

Articles 52 and 53 of the law prescribe the procedure for the submission of request for the approval, as well as the content of the request. The Office of the Council has been appointed to be the competent body to receive the requests.

Articles 54 to 66 of the law define the procedure of the security checkout, which is a condition for the applicant to obtain the approval for the access to classified information. Article 54 of the law prescribes the types of the security checkout, which are defined in relation to the secrecy level of information, for which the request is asked for. For information classified as RESTRICTED and CONFIDENTIAL, the basic security checkout is made, for information classified as TOP SECRET, the complete security checkout is made and for information classified as TOP SECRET, the special security checkout is made.

Article 55 of the law prescribes the bodies competent to make security checkouts. The Security Information Agency is competent for the access to classified information and documents classified as TOP SECRET and SECRET and the Ministry of Internal Affairs is competent for the access to classified information and documents classified as CONFIDENTIAL and RESTRICTED. The Military Security Agency shall make security checkouts for the access to classified information and documents of all levels of secrecy for the persons who need this access in order to perform their functions or work assignments at the Ministry of Defence and the Army of Serbia. The Security Information Agency shall make security checkouts for the access to classified information and documents of all levels of

secrecy for the persons who need this access in order to perform their functions or work assignments at the Security Information Agency. The Ministry of Internal Affairs may also make security checkouts for the access to classified information and documents classified as SECRET for the persons who need this access in order to perform their functions or work assignments at the Ministry of Internal Affairs in addition to the Security Intelligence Agency of the Republic of Serbia.

Articles 57 to 66 of the law determine the purpose of security checkouts, content of security questionnaire for all types of security checkouts, special security checkout, time limits to make security checkouts, issuance of provisional approval before the completion of security checkout and submission of the report about the results of security checkout**.**

The competent body is obliged to make the security checkout within 30 days from the date of the receipt of the questionnaire for the basic security checkout, within 60 days for the complete security checkout and within 90 days for the special security checkout. If the security checkout is not made within the specified time limits, it shall be considered that there is no security risk for classified information of the applicant. The bodies competent to make security checkouts shall submit to the Office of the Council the report on the results of security checkout including the filled in questionnaire and the recommendation for the issuance or revocation of the approval.

Article 67 of the law prescribes that the Office of the Council shall decide on the issuance of the approval by means of a decision, within 15 days from the date of the submission of the report containing the recommendation, namely from the expiration of the time limit to make the security checkout.

If it cannot be determined from the report on the results of the security checkout and the recommendation for the issuance of the approval whether the conditions prescribed by law for the issuance of the approval to natural persons or legal entities have been fulfilled or not, or whether some substantial amendments of the checked out data have taken place after the security checkout, the Office of the Council shall request from the competent body to carry out an additional checkout.

Article 70 of the law precisely defines the reasons why the Office of the Council shall dismiss the request for the issuance of approval for the access to classified information. In accordance with Article 72 of this law, the decision of the Office of the Council is final, although the court protection is foreseen, which is accomplished in the administrative proceedings before the competent court.

Articles 74 to 78 of the law prescribe the expiration of the validity of the approval, extension of the validity of the approval, provisional prohibition of access to classified information and checkout of the approval. The law prescribes the methods on how the validity of the approval shall expire, of which one is by expiration of time, depending on the level of secrecy, whereas the period of three years for the validity of approval had been prescribed for the highest level of secrecy, and the minimum validity is fifteen years.

Article 77 of the law prescribes provisional prohibition of the right to access, in case the disciplinary proceedings had been initiated against the person who obtained the approval for the access to classified information. Article 78 of the law prescribes that the Office of the Council may adopt the decision on the termination of validity of the approval even before the expiration of its validity, namely it may restrict the right of the person to access to classified information designated with a certain secrecy level, if it is found that the person who had been issued the approval shall not use or shall not keep such information in accordance with the law and other regulations. The decision of the Office of the Council is final and the administrative proceedings may be initiated against it.

Article 79 of the law prescribes the procedure for the issuance of the permit for the access to national classified information to a foreign person. The Office of the Council shall only issue to the foreign person the permit for the access to information specified in the international treaty, which the Republic of Serbia had concluded with the foreign country, namely with the international organization.

Articles 80 to 84 of the law prescribe keeping of official records and other data related to the approvals and permits, such as records of security checkouts.
Articles 85 to 97 define the monitoring of the enforcement of this law. Articles 85 and 86 prescribe the internal control. The heads of the public authorities are responsible for the internal control over the enforcement of this law. A special work post for the internal control may be foreseen at the Ministry of Internal Affairs, the Ministry of Defence and the Security Information Agency, and, if necessary, at other bodies as well.
Article 87 of the law prescribes that certain jobs of the enforcement of this law and the external control of the enforcement of this law shall be performed by the Office of the Council, as the agency of the Government having the character of a legal entity. Article 88 prescribes the competence of the Office of the Council, the most important being: monitoring of conditions and provision of the application of standards and other regulations in the field of protection of classified information, care to fulfil the accepted international obligations and concluded international treaties in the field of protection of classified information, making and keeping of the Central Registry of Foreign Classified Information and records of issued approvals and permits, preparation of regulations necessary to enforce the law and other jobs prescribed by law. The proposed solution is in full compliance with the comparative case-law pursuant to which the mentioned jobs are to be within the competence of the state authorities. In the majority of countries it is a specialized agency of the government, as also prescribed by the proposed solution.
Articles 90 to 92 of the law prescribe the conditions for the appointment and the termination of duty of the Director and the Deputy Director of the Office of the Council. The Director of the Office is appointed by the Government for the period of five years, after the provision of the opinion of the National Security Council. The Deputy Director is appointed by the Government, under the proposal of the Director of the Office of the Council. The mentioned officials have the status of civil servants holding positions.
Article 93 of the law prescribes the adoption of the document on internal organization and classification of work posts at the Office of the Council, as well as the security checkout and the increase of salaries of the employed at the Office of the Council.
Articles 94 to 97 of the law prescribe the obligations of the Office of the Council related to foreign classified information, keeping the Central Registry of Foreign Classified Information, submission and receipt of information obtained in the international exchange and the possibilities of exchange of information without the international treaty**.**
Articles 98 to 100 of the law contain the penalty provisions, specifying criminal acts and offence regarding violations of this law.
Articles 101 to 110 of the law contain the transitional and final provisions.
Article 101 of the law prescribes that the existing Office of the National Security Council, which was established in accordance with the Law on the Basics of Organization of Security Services of the Republic of Serbia, shall continue its activities and shall have the expanded competence in compliance with the law, as the Office of the National Council for Security and Protection of Classified Information.
Article 104 of the law specifies the time limit for the adoption of by-laws, which amounts to six months from the date of this law entering into force, in case of the documents to be adopted by the Government, namely it amounts to one year for the documents related to other public authorities.
Article 105 of the law prescribes the time limit of two years for re-examination of the existing designations of classified information.
Article 106 of the law prescribes the time limit of two years, from the date of this law entering into force, for the issuance of the approval in accordance with this law to persons who must have the access to classified information in order to be able to perform their work assignments or functions.
Article 110 prescribes that the law shall enter into force eight days from the date of its publication in the Official Gazette of the Republic of Serbia, and it shall be enforced as from 1

January 2010, in order to adopt the necessary by-laws and that the Office of the Council shall get ready for acting in accordance with its competence specified by this law within the period from the date of the law entering into force to the date of commencement of its enforcement.

IV. ASSESSMENT OF FINANCIAL RESOURCES REQUIRED TO ENFORCE THE LAW

No additional resources need to be allocated in the budget of the Republic of Serbia in 2009 in order to implement this law, in view of the fact that the Office of the National Security Council had been established in accordance with the Law on Basics for the Organization of Security Services of the Republic of Serbia (the Official Gazette of RS, no. 116/07).
In addition, in order to apply this law it would be necessary to allocate the funds in the budget of the Republic of Serbia in 2010, since it had been proposed to start the enforcement of the law as from 1 January 2010. Since the law prescribes the expansion of the competence of the Office of the National Council for Security and Protection of Classified Information, it shall be necessary to increase the number of employees at the Office. However, it should be borne in mind that the largest number of the required personnel shall be taken over from other state authorities performing the jobs in the field of classified information (the Ministry of Defence, the Ministry of Foreign Affairs, the Security Information Agency, the Military Intelligence Agency, the Military Security Agency, etc.), so there shall be no need for large additional funds.

ANNEX B: Excerpt from the State Secrets Act of the Republic of Estonia, 26 January 1999 (RT 1 1999, 16, 271):

Article 7

The following items of information are state secrets classified as "top secret":

1) the national action plan for action in an emergency situation, a state of emergency or war-time, as described in the national crisis management plan. A medium containing such information shall be classified for fifty years. Classification shall expire upon declaration of an emergency situation, state of emergency or state of war;
(22.01.2003 entered into force 01.03.2003 - RT I 2003, 13, 67)

2) Methods and tactics for collection of information by the Security Police Board and the Information Board in the manner provided for in §§ 25 and 26 of the Security Authorities Act, and information on the technical equipment used thereby exclusively for the collection of information and the technical equipment specially adapted for such purposes, except for the methods and tactics described in clause 6 (9) of this Act. A medium containing such information shall be classified for fifty years;
(19.05.2004 entered into force 01.07.2004 - RT I 2004, 46, 329)

3) surveillance exercised by the Security Police Board in co-operation with the police and security authorities of foreign states and information exchanged in the course thereof and the collection of information by the Security Police Board or the Information Board in the manner provided for in §§ 25 and 26 of the Security Authorities Act which is done in co-operation with the security authorities of foreign states and information exchanged in the course thereof. A medium containing such information shall be classified for fifty years;
(20.12.2000 entered into force 01.03.2001 - RT I 2001, 7, 17)

4) electronic databases compiled of information collected in the course of surveillance by the Security Police Board and information collected by the Security Police Board or the Information Board in the manner provided for in §§ 25 and 26 of the Security Authorities Act and information concerning such databases. A medium containing such information shall be classified for fifty years;
(20.12.2000 entered into force 01.03.2001 - RT I 2001, 7, 17)

5) persons and undercover agents recruited for permanent secret co-operation by the General Staff of the Defence Forces, the Information Board and the Security Police Board and the personal data of such persons and agents. A medium containing such information shall be classified for seventy-five years. Classification shall expire if twenty years have passed since the death of a person specified in this clause but not more than fifty years since classification of the medium;
(20.12.2000 entered into force 01.03.2001 - RT I 2001, 7, 17)

6) the connection with the Security Police Board of cover organisations founded on the initiative of the Security Police Board in the course of surveillance and impersonation of a person, agency or body necessary for the performance of

functions of the Security Police Board or the Information Board. A medium containing such information shall be classified for fifty years. Classification shall expire upon use of such information in criminal proceedings;
(20.12.2000 entered into force 01.03.2001 - RT I 2001, 7, 17)

7) information concerning the location of the cryptographic information system of the Security Police Board and the Information Board, and the system configuration, equipment configuration, capacity and other parameters thereof. A medium containing such information shall be classified for fifteen years;
(20.12.2000 entered into force 01.03.2001 - RT I 2001, 7, 17)

8) methods and means used to organise and verify INFOSEC and special telecommunications services. A medium containing such information shall be classified for thirty years.
(12.02.2003 entered into force 01.04.2003 - RT I 2003, 23, 147)")

ANNEX C: Excerpt from the Classified Information Protection Act of the Republic of Poland, 22 January 1999 (RT 1 1999, 16, 271):

Annex No 1:

State Secret Classified Information ("I. Information classified "top secret.")

1. Information concerning external military threats to the security of the state; defence plans and forecasts and the decisions and tasks resulting there from.

2. The structure, organisation and functioning of the system for governing the state and commanding the Armed Forces in times of threat to the state and in wartime.

3. The location, equipment, protective potential and organisation of the system for defending the command centres from which the state is to be governed and the Armed Forces commanded in times of threat to the state and in wartime.

4. The organisation and functioning of the communications systems for governing the state and commanding the Armed Forces during times of increased defence readiness and in wartime.

5. The central mobilisation programme for the national economy.

6. Information concerning the planning, organisation and functioning of the Armed Forces' mobilisation deployment plan.

7. The detailed structure of the Armed Forces, likewise of wartime military districts and types of force.

8. Information concerning: the Armed Forces' combat effectiveness; the various military districts and types of force; and the potential enemy in the forecast areas and directions of warfare.

9. The combat tasks of the Armed Forces and operational groupings.

10. The organisation and functioning of the national air and anti-aircraft defence system.

11. The organisation, deployment, tasks and operational capacity of the radio-electronic reconnaissance and combat system.

12. The planning and execution of projects concerned with operational camouflaging of forces.

13. The planning, execution and findings of scientific research and research-and development projects of special importance to national defence and security.

14. Passwords and codes giving access to facilities in which or with the aid of which information classified "top secret" is stored, processed and transmitted.

15. The communications systems planned, organised and maintained by the communications service reporting to the ministers responsible for internal affairs and public administration, to the Minister of Defence and to the Chief of the Office for State Security.

16. The organisation, functioning, security arrangements and facilities for cryptographic protection of the transmission of information classified "top secret", likewise coded messages secured by code algorithms for protecting information accorded that secrecy classification.

17. The organisation, forms and operational work methods of the state bodies, services and institutions authorised to engage in operational-reconnaissance activities.

18. The detailed directions of operational work and interests of the state security services.

19. The detailed organisational and manpower structure of those entities and structures within the state bodies, services and institutions referred to in item 17 which engage in operational-reconnaissance activities, likewise systems for registering information relating to the civilian and military personnel of the said entities and structures.

20. The particulars which reveal or are capable of revealing the identity of members of the civilian and military personnel authorised to engage in operational-reconnaissance activities and employed in the state bodies, services and organisations referred to in item 17.

21. The particulars which reveal or are capable of revealing the identity of those persons who, while not members of the civilian and military personnel of the state bodies, services and organisations referred to in item 17, have assisted the said structures in their operational-reconnaissance activities.

22. Information relating to those documents which prevent the disclosure of particulars by which the identity of members of the civilian or military personnel of the state bodies, services or institutions referred to in item 17 might be established or means employed by them in their operational-reconnaissance work identified.

23. Information relating to the following investigative techniques the use of which is permitted by statutes: technical means of covert intelligence gathering and evidence recording; surveillance of correspondence; controlled purchase; and covertly monitored dispatch.

24. Plans concerning the procurement of special investigative-technique equipment and stocks of the same at the state bodies, services and institutions referred to in item 17.

25. Intelligence and things secured by applying technical means of covert intelligence gathering and evidence recording and through surveillance of correspondence.

26. Information relating to operational-reconnaissance activities--whether planned, in progress or executed--of the state bodies, services and institutions referred to in item 17, likewise such intelligence and objects secured through those activities by which the persons who have assisted the said bodies, services and institutions in their operational reconnaissance activities might be identified.

27. Reports, bulletins, information and statistical data relating to operational activities of the state bodies, services and institutions referred to in item 17.

28. The management of budgetary funds and state property assigned to special purposes.

29. The organisation, functioning and technical means of radio-counterintelligence protection of state security.

30. The classified information accorded the "TOP SECRET" or an equivalent secrecy classification which is exchanged between the Republic of Poland and the North Atlantic Treaty Organisation, European Union, Western European Union and other international organisations and states."