fficial Gazette of the Republic of Serbia, No. 104/2009.

Based on Article 112, paragraph 1, item 2 of the Constitution of the Republic of Serbia, I issue the following

DECREE
promulgating
the Law on Classified Information

The Law on Classified Information passed by the National Assembly of the Republic of Serbia on 11 December 2009 during the Second Session of its Second Regular Sitting for the year 2009 is hereby promulgated.

Ref. No. 190
Belgrade, 16 December 2009

Boris Tadić, sgd.
President of the Republic

THE LAW
ON
CLASSIFIED INFORMATION

I. GENERAL PROVISIONS

Subject of the Law
Article 1

This law shall regulate the unified system of determination and protection of classified information of interest to the national and public security, defense, internal and foreign affairs of the Republic of Serbia, protection of foreign classified information, access to classified information and termination of its classification, competence of the authorities and supervision of the enforcement of this law, as well as the responsibility for non-fulfillment of obligations referred to in this law and other issues of importance for the protection of information classification.

Definitions
Article 2

Within the meaning of this law:
1) *information of interest to the Republic of Serbia* is any information or document managed by the public authorities which relates to the territorial integrity and sovereignty, protection of constitutional system, human and minority rights and freedoms, national and public security, defense, internal and foreign affairs;
2) *classified information* is any information of interest to the Republic of Serbia which has been identified and designated with a certain classification level by law, other regulation or a decision of the competent body adopted pursuant to law;
3) *foreign classified information* is any information entrusted to the Republic of Serbia by a foreign country or an international organization under the provision it shall be kept classified, as well as classified information resulting from the cooperation between the Republic of Serbia and other

countries, international organizations and other international entities, in compliance with an international agreement concluded between the Republic of Serbia and a foreign country, international organization or other international entity;
4) *document* is any data storage medium (paper, magnetic or optical media, diskette, USB memory, smart card, compact disc, microfilm, video and audio recordings, etc.), on which classified information has been recorded or memorized;
5) *determination of classified information* is a procedure under which information is determined to be classified in accordance with this law, and for which the level and duration of classification is established;
6*) designation of classification level* is marking of classified information with the following levels: TOP SECRET , SECRET, CONFIDENTIAL or RESTRICTED;
7) *public authority* is a state body, a body of the territorial autonomy, a body of the local self-government unit, an organization entrusted with exercising public powers, as well as the legal person established by the state body, or a body financed entirely or predominantly from the budget which deals with classified information, or the body which generates, obtains, keeps, uses, exchanges or processes classified information in some other manner;
8) *security vetting* is a procedure conducted by the competent body prior to the issuance of a personnel security clearance for access to classified information in order to collect information on possible security risks and obstacles with respect to reliability for access to classified information;
9) *damage* is a violation of the interests of the Republic of Serbia resulting from unauthorized access, disclosure, destruction and misuse of classified information or from some other action of processing classified information and foreign classified information;
10) *security officer* is a natural person or an organizational unit of the public authority which takes measures for the protection of classified information in accordance with the provisions of this law (hereinafter:“ the security officer”);
11) *user of classified information* is a citizen of the Republic of Serbia or the legal person having the seat in the Republic of Serbia which has been issued a security clearance by the competent body, or the foreign natural or legal person which has been issued a security permit for access to classified information on the basis of a concluded international agreement, as well as an official of the public authority who, under this law, has the right to access and use classified information without the issuance of personnel security clearance;
12) *security risk* is an actual possibility of disrupting the security of classified information;
13) *protection measures* are general and special measures taken in order to prevent the occurrence of damage, or those relating to the achievement of the administrative security, information and telecommunication security, personal and physical security of classified information and foreign classified information.

Information not Considered Classified
Article 3

Information shall not be considered classified if it has been designated as classified for concealment of a criminal offence, transgression of powers or abuse of official duty or for any other illegal action or conduct of the public authority.

Right of Access
Article 4

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

Purpose of Collection
Article 5

Classified information may only be used for the purpose it has been collected for, pursuant to law.

Safekeeping and Use of Classified Information
Article 6

Classified information shall be kept safe and used in accordance with the protection measures prescribed by this law, regulation adopted on the grounds of this law and international agreements.

The person who uses classified information or the person who has learnt its content shall be under obligation to keep such information safe regardless of the manner in which he/she has become aware of it.

The obligation referred to in paragraph 2 of this Article shall remain in force upon the termination of function or termination of employment or upon the termination of the performance of duty or membership in the public authority or a relevant body.

Protection of Business Secrets and Other Secrets
Article 7

The protection of business secrets and other secrets shall be regulated by specific laws.

II. DETERMINATION OF CLASSIFIED INFORMATION

Information that May be Determined to be Classified
Article 8

Any information of interest to the Republic of Serbia, whose disclosure to an unauthorized person would cause damage, may be determined to be classified, if the need for the protection of the interests of the Republic of Serbia prevails over the interest in the free access to information of public importance.

The information referred to in paragraph 1 of this Article shall particularly concern:
1) the national security of the Republic of Serbia, public security, or defense, 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, designs, plans and structures relating to the information in items 1) and 2) of this paragraph;
4) scientific, research, technological, economic and financial affairs relating to the information referred to in items 1 and 2 of this paragraph.

Person Authorized to Determine Classified Information
Article 9

An authorized person shall determine classified information under the conditions and in the manner established by this law.

The authorized persons are as follows:
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 or by the regulation adopted on the grounds of law, or who has been authorized to do so in writing by the head of the public authority;
6) a person employed by the public authority who has been authorized in writing by the head of the public authority.

The authorized persons referred to in paragraph 2, items 5 and 6 of this Article may not transfer their authorizations to other persons.

Procedure for Determining Classified Information
Article 10

The authorized person referred to in Article 9 paragraph 2 of this law shall determine the classified information as it is generated or when the public authority begins performing an activity resulting in the generation of classified information.

With the exception of paragraph 1 of this Article, the authorized person may also determine classified information subsequently, after the criteria defined by this law have been fulfilled.

When determining classified information, the authorized person shall assess possible damage to the interests of the Republic of Serbia.

A person employed by the public authority or a person performing particular activities within the public authority shall be obliged, within the scope of his/her work duties or of his/her authorizations, to inform the authorized person of the information which may be determined to be classified.

Decision to Determine Classification Level
Article 11

The decision to determine classification level shall be taken on the basis of the assessment referred to in Article 10 paragraph 3 of this law, and the documents shall be marked with a classification level as provided by this law (hereinafter: the classification marking).

When determining the information classification level, the authorized person shall determine the lowest classification level which shall prevent the occurrence of damage to the interests of the Republic of Serbia.

If a document contains information that may be designated with different classification levels, the authorized person shall designate the document with a higher classification level in relation to such levels of classification.

The decision referred to in paragraph 1 of this Article shall be adopted in the written form along with the statement of reasons.

Special Cases of Determination and Designation of Classified Information
Article 12

Information generated through consolidation or linking of information which is not inherently classified shall be determined to be classified by the authorized person, if the information consolidated

or linked in such a manner constitutes the information that needs to be protected for the reasons established by this law.

A document containing information that has already been determined to be classified with different classification levels and classification time limits shall be designated with a higher classification level and a longer classification time limit of the contained information in relation to the above information.

If a minor part of the document contains classified information, it shall be singled out and enclosed with the document as a separate attachment designated with a classification marking.

Classification Markings
Article 13

The document containing classified information shall be designated with the following:
1) marking of classification level;
2) method of classification termination;
3) information on the authorized person;
4) information on the public authority.

Except for paragraph 1 of this Article information shall be considered classified, if the document containing such information is designated with a classification level only.

The Government shall prescribe the method and the procedure for marking classification of information or documents.

Classification Levels and Information Content
Article 14

The information referred to in Article 8 of this law shall have one of the following classification levels:
1) TOP SECRET which is determined in order to prevent the occurrence of irreparable damage to the interests of the Republic of Serbia;
2) SECRET which is determined in order to prevent the occurrence of grave damage to the interests of the Republic of Serbia;
3) CONFIDENTIAL which is determined in order to prevent the occurrence of damage to the interests of the Republic of Serbia;
4) RESTRICTED which is determined in order to prevent the occurrence of damage to the activities or to the performance of duties and tasks of the public authority that has defined them.

Only classification levels referred to in paragraph 1 of this Article may be used for determining information classification levels.

More detailed criteria for determining the TOP SECRET and SECRET classification levels shall be established by the Government based on the previously obtained opinion of the National Security Council.

More detailed criteria for determining the CONFIDENTIAL and RESTRICTED classification levels shall be established by the Government at the proposal of the competent minister or the head of the public authority.

Designation of Foreign Classified Information
Article 15

A document containing foreign classified information shall retain the classification level marking it has been designated with in the foreign country or by an international organization.

When designating classification levels of documents, apart from the terms referred to in Article 14 of this law, the classification level markings in English may be used for documents intended for cooperation with foreign countries whose disclosure to an unauthorized person would cause damage, namely:

1) TOP SECRET classification level marking shall correspond to „ДРЖАВНА ТАЈНА”/ „DRŽAVNA TAJNA“ classification level marking;
2) SECRET classification level marking shall correspond to „СТРОГО ПОВЕРЉИВО”/ „STROGO POVERLJIVO“ classification level marking;
3) CONFIDENTIAL classification level marking shall correspond to „ПОВЕРЉИВО”/ „POVERLJIVO“ classification level marking;
4) RESTRICTED classification level marking shall correspond to „ИНТЕРНО”/„INTERNO“ classification level marking.

Time Limitation on Information Classification
Article 16

Classification of information shall be terminated:
1) on the date determined in the document containing classified information;
2) upon the occurrence of the particular event determined in the document containing classified information;
3) upon the expiration of the time limit prescribed by law;
4) upon the revocation of classification;
5) if information is made available to the public.

The authorized person may change the defined method for terminating classification of information, if there are justified reasons to do so, in accordance with the law.

The authorized person shall be obliged to immediately send a written notification of the above change to the public authorities and the persons who have received classified information or have access to such classified information.

Termination of Classification on Specified Date
Article 17

If the authorized person establishes during the procedure for determining classification that the reasons for which information has been declared classified shall cease to exist on the specified date, the classification termination date shall be determined and marked in the document containing such information.

Termination of Classification upon Occurrence of Particular Event
Article 18

If the authorized person establishes in the procedure for determining classified information that upon the occurrence of the particular event the reasons for which some information has been declared classified shall cease to exist, he/or shall establish that classification shall be terminated upon the occurrence of such an event, and mark the same in the document containing such information.

Termination of Classification upon Expiration of Time Limit
Article 19

If the termination of classification has not been determined in accordance with Articles 17 and 18 of this law, classification shall be terminated upon the expiration of the time limit established by this law.

The statutory time limit for the termination of information classification referred to in paragraph 1 of his Article shall be determined according to the following classification level:
1) for classified information marked with the TOP SECRET level - 30 years;
2) for classified information marked with the SECRET level - 15 years;
3) for classified information marked with the CONFIDENTIAL level - five years;
4) for classified information marked with the RESTRICTED level - two years.

The time limits referred to in paragraph 2 of this Article shall begin running from the date of determining classification of information.

Extension of Information Classification Period
Article 20

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

In addition to the authorized person referred to in paragraph 1 of this Article, the Government may also extend the time limit for keeping the classification of information in the following cases:
1) if their disclosure would have irreparable, grave and harmful implications for the national security and for the particularly important state, political, economic or military interests of the Republic of Serbia;
2) if it is stipulated by an international agreement or required by international obligations of the Republic of Serbia;
3) if their disclosure would have irreparable and grave implications for fundamental human and civil rights of one or more persons, or if it would threaten the security of one or more persons.

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

Revocation of Classification
Article 21

During the procedure for revoking classification of information it is established that information shall cease to be classified before the expiration of the time limit referred to in Articles 17 to 20 of this law.

The decision to revoke classification of information shall be adopted if the facts and circumstances occur due to which such information will cease to be of interest to the Republic of Serbia.

The decision referred to in paragraph 2 of this Article shall be taken on the grounds of the periodical assessment of classification, proposal for revocation or based on the decision of the competent state authority.

Periodical Assessment of Classification
Article 22

The authorized person shall carry out the periodical assessment of classification, on the basis of which he/she may revoke classification, namely:
1) for the information marked with the TOP SECRET classification level at least once in ten years;
2) for the information marked with the SECRET classification level at least once in five years;
3) for the information marked with the CONFIDENTIAL classification level at least once in three years;
4) for the information marked with the RESTRICTED classification level at least once a year.

If it is established that there exist reasons referred to in Article 21 paragraph 2 of this law, the authorized person shall without delay adopt the decision to revoke classification which must include the statement of reasons.

Proposal for Revocation of Classification
Article 23

The user of classified information may propose to the authorized person to revoke classification of information.

The authorized person shall be obliged to consider the proposal referred to in paragraph 1 of this Article and inform the proposer of his/her decision.

Revocation of Classification during the Control Procedure
Article 24

During the control procedure, the Office of the Council on National Security and Protection of Classified Information (hereinafter: the Council Office) may request the authorized person to carry out an extraordinary assessment of information classification and adopt the decision to revoke classification on its own based on such an assessment.

Revocation of Classification Based on the Decision of the Competent Authority
Article 25

The authorized person of the public authority shall revoke the classification of information or the classification of a document containing classified information, and shall enable the applicant to exercise the right of access to classified information based on the decision of the Commissioner for Information of Public Importance and Personal Data Protection in the appeal proceedings, or based on the decision of the competent court in the suit proceedings pursuant to the law regulating free access to information of public importance and the law governing personal data protection.

Revocation of Classification in the Public Interest
Article 26

The National Assembly, the President of the Republic and the Government may revoke a classification marking of certain documents, regardless of the classification level, if such revocation is in the public interest or is due to the fulfillment of international obligations.

Change in Classification Level and Duration
Article 27

The change in the information classification level shall mean designating information with a higher or a lower level of classification than the classification level such information has had until that point, before the expiration of the time limit referred to in Articles 17 to 20 of this law.

The change in the classification level and duration shall be made by applying the provisions referred to in Articles 21 to 24 and Article 26 of this law accordingly.

Notification of Change in Classification Level and Revocation of Classification
Article 28

The authorized person shall immediately notify in writing the users of classified information and the persons having access to such information of the change in the classification level and duration, as well as of the revocation of classification.

Foreign Classified Information
Article 29

The change in the classification level and duration, as well as the revocation of classification of foreign information, shall be made in accordance with a concluded international agreement and established international obligations.

III. MEASURES FOR PROTECTION OF CLASSIFIED INFORMATION

Criteria for Protection of Classified Information
Article 30

The public authority shall, pursuant to this law and the regulations adopted on the basis of this law, establish a system of procedures and measures for the protection of classified information according to the following criteria:

1) classification level;
2) nature of the document containing classified information;
3) risk assessment of the security of classified information.

Types of Protection Measures
Article 31

The public authority shall implement general and special protection measures in accordance with the law and the regulation adopted on the grounds of this law in order to protect classified information in its possession.

General Protection Measures
Article 32

General protection measures relating to classified information shall include:

1) determination of classification level;
2) risk assessment of the security of classified information;
3) determination of method of use and handling of classified information;
4) appointment of the person responsible for safekeeping, use, exchange and other activities relating to the processing of classified information;

5) appointment of security officer, including also his/her security vetting, depending on the information classification level;
6) determination of special security zones, buildings and premises intended for the protection of classified information and foreign classified information;
7) supervision of handling of classified information;
8) measures for physical security and technical protection of classified information, including fitting and installation of technical means of protection, establishment of secure zone and protection outside secure zone;
9) protection measures for information-telecommunications systems;
10) crypto protection measures;
11) protective mode of operation for work and formational posts within the document on internal organization and work post classification;
12) establishment of special educational and training programs needed for the performance of activities for the protection of classified information and foreign classified information;
13) other general measures defined by law.

Special Protection Measures
Article 33

With the aim to achieve an efficient implementation of general measures for the protection of classified information referred to in Article 32 of this law, special measures for the protection of classified information shall be defined in a by-law to be adopted by the Government.

Some of the special protection measures may be more precisely defined in a document issued by the competent minister or by the head of a specific organization in compliance with a by-law to be adopted by the Government referred to in paragraph 1 of this Article.

Obligations of the Security Officer
Article 34

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

Safekeeping, Transfer and Transmission of Classified Information
Article 35

Classified information shall be kept safe in a manner that allows access to such information to the authorized users only.

Classified information may be transferred and transmitted outside the premises of the public authority only on condition that this is in compliance with the prescribed security measures and procedures, which ensure that classified information shall only be obtained by the person who has a personnel security clearance for access to classified information and who is entitled to obtain it (“NEED TO KNOW”).

When transferring and transmitting classified information outside the premises of the public authority, the procedures and protection measures shall be determined according to the classification level of such information, in accordance with the law and the regulation adopted on the grounds of the law.

The transfer and the transmission of classified information by means of telecommunications and information technology shall be carried out with the obligatory implementation of the prescribed crypto protection measures.

The implementation of crypto protection measures when transferring and transmitting classified information as referred in paragraphs 3 and 4 of this Article shall be carried out according to the law.

Obligation of Notification in Case of Loss, Theft, Damage, Destruction or Unauthorized Disclosure of Classified Information and Foreign Classified Information
Article 36

If it is learned that there has been a loss, theft, damage, destruction or unauthorized disclosure of classified information and foreign classified information, the official, the employee or the person performing tasks within the public authority, shall without delay notify the authorized person of the public authority of such an event.

The person referred to in Article 35 paragraph 2 of this law, who establishes that there has been a loss, theft, damage, destruction or unauthorized disclosure of classified information and foreign classified information in the course of transferring and transmitting classified information outside the premises of the public authority, shall immediately notify the authorized person of the public authority who has transferred or transmitted classified information and foreign classified information to him/her.

The authorized person shall be obliged to take without delay all necessary measures to establish the circumstances that have brought about the theft, damage, destruction or unauthorized disclosure of classified information and foreign classified information, make an estimate of the damage caused, as well as to take necessary measures with the aim to undo the damage and prevent a repetition of the theft, damage, destruction or unauthorized disclosure of classified information and foreign classified information.

If such case as referred to in paragraph 3 of this Article, the authorized person shall notify the Council Office of the taken measures.

IV. ACCESS TO CLASSIFIED INFORMATION

Access to Classified Information without Personnel Security Clearance
Article 37

The President of the National Assembly, the President of the Republic and the Prime Minister shall have access to classified information, and use information and documents of any classification level without having to be issued a personnel security clearance on the basis of their respective functions and with the aim to perform the activities within their respective remits.

Access to Classified Information without Security Vetting, and Special Authorizations and Duties
Article 38

The public authorities elected by the National Assembly, the heads of the public authorities elected by the National Assembly, judges of the Constitutional Court and other judges shall be authorized to access information of all classification levels needed for performing the activities within their respective remits without a security vetting.

Exceptionally, the persons referred to in paragraph 1 of this Article shall be entitled to access classified information marked with the TOP SECRET and SECRET classification level on condition they have undergone a prior security vetting referred to in Article 53, item 2) and 3) of this law, if this is required for performing tasks within their respective remits and if such information relates to the following:

1) actions relating to prevention, discovery, investigation and prosecution of criminal offences conducted by the competent public authorities until the completion of the investigation or prosecution;
2) method of implementation of special procedures and measures for obtaining security information and intelligence in a specific case;
3) members of the ministry competent for internal affairs and security sevices with concealed identity, as long as this is necessary for the protection of vital interests of these persons or the members of their families (life, health and bodily integrity);
4) identity of the current and former associates of the security services or third parties as long as this is necessary for the protection of vital interests of these persons or the members of their families (life, health and bodily integrity).

The persons with access to classified information in accordance with this law shall be authorized and obligated to protect classified information learnt in the procedure they regularly conduct, from everybody in every appropriate manner, and to personnaly handle the classified information referred to in paragraph 2 of this Article.

Right of Access of the Members of the Competent Committee of the National Assembly
Article 39

The members of the Committee of the National Assembly competent for the supervision and control within the defense and security sector shall have the right of access and examination of classified information relating to the performance of such supervision and control functions, pursuant to the law.

Right of Access to the "RESTRICTED" Classified Information Level
Article 40

Officials, employees or persons performing tasks for the public authorities shall have the right of access to the "RESTRICTED" classified information level.

The persons referred to in paragraph 1 of this Article shall sign a statement, confirming that they shall handle classified information in accordance with the law and other regulations.

Access to Foreign Classified Information
Article 41

The access to foreign classified information shall be made in accordance with this law, regulations adopted on the grounds of this law or in accordance with an international agreement the Republic of Serbia has concluded with a foreign country, and international organization or any other international entity.

Natural and Legal Persons as Users of Classified Information
Article 42

Natural and legal persons - users of classified information shall be entitled to access classified information which is indispensable in performing tasks within their scope of activities, as well as

specified in a personnel or facility security clearance or a security permit for access to classified information according to the classification level.

With the exception of paragraph 1 of this Article, in case of extreme urgency of action, the person who has been issued a personnel or facility security clearance or a security permit for access to classified information of lower classification level may be informed of classified information marked with an immediately higher classification level.

The person referred to in paragraph 2 of this Article shall be obliged to sign a statement, confirming that he/she shall handle the classified information in accordance with the law and other regulations.

Statement and Security Clearance
Article 43

Before issuing a security clearance or a security permit, the person who is issued such a clearance shall sign a statement, confirming that he/she shall handle classified information in accordance with the law and other regulations.

If the person referred to in paragraph 1 of this Article does not sign the statement, the procedure for issuing the security clearance or security permit shall be suspended.

The above written statement shall be an integral part of the documentation based on which the security clearance or security permit has been issued.

Release of Obligation to Keep Classified Information
Article 44

The person who has been issued a security clearance or a security permit may not use the information for other purposes except for those for which such clearance or permit has been issued.

The head of the public authority may, at the request of the competent body, release the person of the obligation to keep classified information by means of a specific decision, which shall also envisage the measures for the protection of its classification, but only for the purposes and within the scope contained in the request of the competent body in accordance with the law.

At the request of the competent body, the head of the public authority may be released of the obligation to keep classified information by the body that has appointed, elected or nominated him/her, and the latter body shall notify the Council Office of such a release of obligation accordingly.

Transmission of Classified Information under Obligation to Keep it Classified
Article 45

Classified information may be transmitted to another public authority on the basis of a written approval by the authorized person of the public authority which has designated such information as classified, unless otherwise provided by a specific law.

Classified information received from the public authority may not be transmitted to another user without an approval of the body which has designated such information as classified, unless otherwise provided by a specific law.

The persons working for the public authority to which classified information referred to in paragraph 1 of this Article has been transmitted shall act in accordance with the provisions of this law, and be under obligation to comply with the classification marking and take measures for the protection of information classification.

Transmission of Classified Information based on the Contractual Relationship
Article 46

The authorized person may transmit classified information to other natural or legal persons, which provide services to the public authority based on the contractual relationship, if:
1) the legal or natural person fulfills organizational and technical conditions for safekeeping classified information according to this law and the regulation adopted on the grounds of this law;
2) security vettings have been carried out and clearances issued for the persons performing contracted activities;
3) the persons referred to in item 2) of this paragraph shall confirm by means of a written statement that they have been briefed on this law and other regulations governing the safekeeping of classified information, and that they shall undertake to handle classified information in accordance with such regulations;
4) the access to classified information is indispensable in implementing the activities stipulated by the contract.

The measures for the protection of classified information resulting from paragraph 1 of this Article must be contained in the contract relating to the implementation of activities concluded between the public authority and the legal or natural person.

The Government shall define in more detail the method and the procedure for determining the level of compliance with the conditions referred to in paragraph 1, item 1) of this Article.

Records on Classified Information Provided to Other Users
Article 47

The security officer of the public authority shall establish and keep updated records on classified information provided to other users outside the public authority.

V. PROCEDURE FOR ISSUING SECURITY CLEARANCES OR SECURITY PERMITS

Conditions for Issuing Personnel Security Clearance to Natural Person
Article 48

The personnel security clearance shall be issued by the competent body determined by this law, on the grounds of a written application submitted by a natural person, if the applicant
1) is a citizen of the Republic of Serbia;
2) is of age;
3) has business capacity;
4) has not been pronounced a non-suspended prison sentence for a criminal offence prosecuted *ex officio*, or for amisdemeanor envisaged by this law;
5) has passed an adequate security vetting.

Conditions for Issuing Facility Security Clearance to Legal Person
Article 49

The facility security clearance shall be issued by the competent body established by this law based on a written application of the legal person submitted through the legal representative, if the applicant
1) has a registered seat in the territory of the Republic of Serbia;
2) performs activities relating to the interests set out in Article 8 of this law;
3) passes an adequate security vetting;
4) is not in the process of liquidation or undergoing a bankruptcy procedure;
5) has not been imposed a penal measure, prohibiting the performance of the activities, or has not been pronounced a penalty, terminating the legal personality or imposed a security measure prohibiting the performance of particular registered activities or operations;
6) regularly pays taxes or contributions.

Issuance of Security Permit to Foreign Person
Article 50

A foreign person shall be issued a security permit by the competent authority if:
1) a foreign person holds an adequate personnel or facility security clearance issued in the country whose citizenship he/she holds, or in which he/she has the seat, or by an international organization such a foreign person is a member of;
2) the obligation to allow access to classified information stems from a concluded international agreement.

Submission of Application
Article 51

An application for issuing a security clearance or a security permit shall be submitted to the Council Office.

If the personnel security clearance is requested by a security officer or another employee of the public authority, the application referred to in paragraph 1 of this Article shall be submitted by the head of the public authority.

If the security clearance is requested for the legal person and the employees of that legal person, the application shall be submitted by the legal representative of the legal person.

The application for issuing a security clearance to the person, who is to have access to classified information for the purpose of performing contracted activities for the public authority, shall be submitted by the public authority the performance of such contracted activities refers to.

Content of Application
Article 52

The application for personnel security clearance submitted by a natural person shall contain: name and surname, place of residence, activities performed, reasons for applying for such a clearance, as well as the information classification level the clearance is requested for.

An application for facility security clearance submitted by the legal person shall contain: the company's name, seat and activities of the legal person, name and surname and place of residence of the legal representative of the legal person, reasons for applying for such a clearance, as well as the information classification level the clearance is requested for.

In addition to the information referred to in paragraph 1 or 2 of this Article, a foreign person shall also submit a security clearance referred to in Article 50 item 1) of this law.

Security Vetting
Article 53

A security vetting shall be carried out for access to and use of classified information depending on the classification level, namely:
1) basic security vetting shall be carried out for the information marked with the RESTRICTED and CONDIFENTIAL classification levels;
2) full security vetting shall be carried out for the information marked with the SECRET classification level;
3) special security vetting shall be carried out for the information marked with the TOP SECRET classification level.

Body in Charge of Security Vetting
Article 54

The security vetting for access to classified information and documents marked with the TOP SECRET and SECRET classification levels shall be carried out by the Security and Information Agency of the Republic of Serbia.

The security vetting for access to classified information and documents marked with the CONFIDENTIAL and RESTRICTED classification levels shall be carried out by the ministry competent for internal affairs.

The security vetting for access to classified information and documents at all classification levels for the persons who need access to classified information and documents in order to perform their functions or work duties at the ministry competent for defense and the Army of Serbia shall be carried out by the Military Security Agency.

With the exception of paragraph 2 of this Article, the security vetting for access to classified information and documents marked with the CONFIDENTIAL and RESTRICTED classification levels for the persons who need access to classified information and documents in order to perform their functions or work duties at the Security and Information Agency, shall be carried out by the Security and Information Agency.

In addition to the body referred to in paragraph 1 of this Article, the security vetting for access to classified information and documents marked with the SECRET classification level for the persons who need access to classified information and documents in order to perform their functions or work duties at the ministry competent for internal affairs, may also be carried out by the ministry competent for internal affairs.

The bodies responsible for the security vetting referred to in paragraphs 1 to 5 of this Article shall be under obligation to cooperate between themselves in the security vetting procedure, in particular in the security vetting procedure for access to classified information marked with the TOP SECRET and SECRET classification levels.

Cooperation with Foreign Countries and International Organizations
Article 55

In the course of the security vetting procedure, the bodies competent for security vetting referred to in Article 54 of this law may cooperate with the bodies of other foreign countries, international organizations and other international entities competent for the security vetting in accordance with an international agreement the Republic of Serbia has concluded with a foreign country, international organization or another international entity, and pursuant to the regulations governing personal data protection in the Republic of Serbia.

Purpose of Security Vetting
Article 56

The security vetting of the applicant shall be carried out to assess a security risk, particularly the one relating to access to and use of classified information.

Within the security vetting the competent body shall assess the data stated in the filled-in questionnaire from a security standpoint.

With respect to the data stated in the security questionnaire, the competent body shall collect personal and other data from the person such data refers to, other public authorities, organizations and persons, registers, records, data bases and data collections kept pursuant to the law.

Security Questionnaire
Article 57

In order to carry out the security vetting, the Council Office shall submit a security questionnaire to the applicant.

The applicant shall fill in the basic security questionnaire, and if the personnel security clearance is requested for classified information marked with the TOP SECRET and SECRET classification levels, the applicant shall also fill in a special security questionnaire.

The questionnaire filled in and signed by the applicant shall at the same time represent a written consent to carry out the security vetting and shall be marked with the RESTRICTED classification level.

Basic Security Questionnaire for Natural Persons
Article 58

The following information on the applicant shall be provided in the basic security questionnaire:
1) name and surname, as well as previous names and surnames;
2) single personal identification numbers;
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 on the persons living in the joint household with the person the security questionnaire refers to (their names and surnames along with previous names and surnames, dates of birth, as well as their relationship with the person undergoing the security vetting);

8) name and surname, date of birth and residence address of the relative up to the second degree of kinship in the direct line and up to the first degree of kinship in the lateral line, adopted persons, guardians, step-fathers, step-mothers, or foster parents;
9) educational qualifications and occupation;
10) information on former employments;
11) information relating to military service;
12) information on criminal and misdemeanor sanctions, and criminal and misdemeanor proceedings in progress;
13) medical data relating to addictive illnesses (alcohol, addictive drug, etc.), or mental illness;
14) contacts with foreign security services and intelligence services;
15) disciplinary procedures and imposed disciplinary measures;
16) information on membership or participation in the activities of organizations, whose activities and objectives are prohibited;
17) information on liability for violating regulations relating to information classification;
18) information on property rights or other real right to real estate, information on property right over other assets entered in the public registry, as well as information on annual tax on total income of citizens for the previous year;
19) previous security vettings.

Basic Security Questionnaire for Legal Persons
Article 59

The following information on the applicant shall be filled in the basic security questionnaire for legal persons:
1) name and seat of the company, as well as previous names and seats of the company;
2) single identification number and tax identification number;
3) name and surname of the legal representative;
4) date and place of establishment;
5) information on organizational units, branches, dependent companies and other forms of association;
6) origin of initial capital including changes that occurred within the last three years;
7) number of employees;
8) number of employees personnel security clearances are requested for and type of tasks performed by them;
9) information on convictions for criminal offences, economic offences and misdemeanors of the legal person and persons in charge within the legal person, as well as information on the proceedings for criminal offences, economic offences or misdemeanors against the legal person in progress;
10) information on contacts with foreign security services and intelligence services;
11) information on participation in the activities of organizations whose activities and objectives are prohibited;
12) information on liability for violating regulations relating to information classification;
13) information on previous security vettings;
14) information on property rights or other real right to real estate, information on property right over other assets entered in the public registry, as well as information on the annual financial statement for the previous year in accordance with the law governing accounting and auditing.

The legal representative of the legal person shall also submit a filled-in basic security questionnaire for the natural person together with the filled-in questionnaire referred to in paragraph 1.

Special Security Questionnaire
Article 60

In addition to the basic security questionnaire, the special security questionnaire shall also be filled in for the security vetting set out in Article 53, items 2) and 3) of this law.

The following information shall be provided in the special security questionnaire:
1) information on service in foreign armies and paramilitary formations;
2) other information and facts, apart from the information stated in Articles 58 and 59, which may cause natural or legal persons to be susceptible to influences and pressures which constitute a security risk;
3) information on debts resulting from financial borrowing or undertaken guarantees.

Subject of Security Vetting and Questionnaire Form
Article 61

The information from the questionnaires referred to in Articles 58 to 60 of this law shall be the subject of an adequate security vetting.

The forms of the questionnaires referred to in paragraph 1 of this Article shall be prescribed by the Government at the proposal of the Council Office.

Special Security Vetting
Article 62

A special security vetting shall be carried out when the issuance of the personnel security clearance or the permit is requested for classified information marked with the TOP SECRET classification level.

Such a special security vetting shall also include, apart from checking out the facts within a full security vetting, the checkout of facts, circumstances and events in the applicant's private life covering the period of the last ten years at least, starting from the date of submission of the application for issuing a personnel security clearance. In case such a checkout proves the existence of different facts, circumstances and events in the applicant's private life than those stated, this would constitute the grounds for suspicion about his/her trustworthiness and reliability, especially if his/her activities are contrary to the interests of the Republic of Serbia, or if he/she is connected to foreign persons who may threaten the security and international interests of the Republic of Serbia.

Time Limits for Carrying Out Security Vettings
Article 63

The competent body shall be under obligation to carry out the security vetting from the date of receipt of the filled-in questionnaire within the following time limits:
1) up to 30 days for a basic security vetting;
2) up to 60 days for a full security vetting;
3) up to 90 days for a special security vetting.

Exceptionally, if there are justified reasons, the time limits referred to in paragraph 1 items 2) and 3) of this Article may be extended for the periods established in these items at the most.

In case as referred to in paragraph 2 of this Article, the competent body shall be obliged to inform the head of the public authority which has submitted an application for personnel security clearance, as well as the Council Office of the extension of the time limit.

If the security vetting is not carried out within the time limits specified in paragraphs 1 and 2 of this Article, it shall be deemed that there is no security risk for access to the applicant's classified information.

Provisional Security Clearance
Article 64

In order to perform urgent operations and assignments of the public authority, and with the aim to prevent or undo the damage, the Director of the Council Office may exceptionally, even before the completion of the security vetting, issue the person a provisional security clearance for access to particular classified information, if it is assessed, based on the examination of the submitted security questionnaire, that there is no suspicion in respect to security.

The person referred to in paragraph 1 of this Article shall be obliged to confirm by means of a written statement that he/she shall handle classified information entrusted to him/her in accordance with this law and other regulations governing safekeeping and handling of classified information.

The provisional security clearance referred to in paragraph 1 of this Article shall be valid until the date of the completion of the procedure for issuing a security clearance.

Submission of Report on Security Vetting Results
Article 65

The bodies competent for carrying out the security vetting referred to in Article 54 of this law, shall submit to the Council Office a report on the results of such a security vetting or a special security vetting, including the filled-in security questionnaire with a recommendation to issue or deny a clearance.

The sources of such a security vetting shall not be stated in the report referred to in paragraph 1 of this Article.

The report and recommendation referred to in paragraph 1 of this Article shall be marked with the CONFIDENTIAL classification level.

Decision and Additional Vetting
Article 66

The Council Office shall resolve to issue a personnel security clearance by means of decision, within 15 days from the date of submitting the report containing the recommendation referred to in Article 65, paragraph 1 of this law, namely from the expiration of the time limit for carrying out the security vetting referred to in Article 63 of this law.

If the report is incomplete or submitted without a recommendation, the Council Office shall issue a decision on the basis of the submitted report.

Exceptionally, if it cannot be determined on the basis of the report on the security vetting results and the recommendation for issuing a clearance whether the statutory conditions for issuing a personal or

facility security clearance to the natural or legal person have been fulfilled or not, or some substantial changes of the checked out data have occurred after the security vetting which may have an impact on the personnel security clearance issuance, the Council Office shall request the competent body referred to in Article 54 of this law to carry out an additional vetting or to provide an appendix to the report and prepare a new recommendation within a subsequent period of 30 days at the latest .

Exceptions
Article 67

As an exception from Article 66 of this law, the decision to issue a personnel security clearance for access to classified information managed by the security service shall be adopted by the head of the service referred to in Article 54 paragraphs 3 and 4 of this law, with respect to 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.

Submission of Decision
Article 68

The Council Office shall submit the decision to the head of the public authority who has requested the issuance of the personnel security clearance and to the person such a clearance has been requested for.

Refusal of Application
Article 69

The Council Office shall refuse an application for issuing a security clearance by means of decision, if it is established, based on the report on the security vetting or on the additional security vetting that:
1) the applicant has stated untrue and incomplete information in the basic or special security questionnaire;
2) the applicant does not meet the requirements for issuing a security clearance or permit referred to in Articles 48 to 50 of this law;
3) the applicant has not provided the conditions to take prescribed measures to protect classified information;
4) there is a security risk from the access and use of the applicant's classified information.

The statement of reasons of the decision on the refusal to issue the security clearance shall contain neither the information considered classified within the meaning of this law nor shall state the sources of the security vetting.

Adequate Application
Article 70

The provisions of the law regulating the general administrative procedure shall be applied to the procedure for issuing a security clearance or permit, unless otherwise provided by this law.

Administrative Dispute
Article 71

A complaint against the decision of the Council Office referred to in Article 66, paragraph 1 of this law may be referred to the minister competent for the judiciary.

The provisions of the law governing the administrative proceedings shall be applied when deciding such a complaint.

The decision issued by the minister responsible for the judiciary shall be final and administrative dispute may be initiated against it.

Content, Form and Submission of Clearance
Article 72

The content, form and method of submission of a security clearance shall be prescribed by the Government at the proposal of the Council Office.

The Council Office shall submit the clearance and brief the user on the prescribed conditions for handling classified information, as well as of legal and other consequences of its unauthorized use.

When receiving the clearance, the user shall sign the same, as well as a statement that he/she has been briefed on the provisions of the law and other regulations governing the protection of classified information and that he/she shall use classified information in accordance with the law and other regulations.

Termination of Security Clearance Validity
Article 73

The clearance validity shall terminate:
1) upon the expiration of the period it has 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 tasks within the scope of activities of the person referred to in Article 40 of this law;
4) on the grounds of the decision adopted by the Council Office in the procedure for checking out the issued security clearance;
5) upon the death of the natural person or termination of the legal person that has been issued a personnel security clearance.

Termination of Security Clearance Validity
upon Expiry of Specified Period
Article 74

A security clearance issued for information and documents marked with TOP SECRET classification level shall be valid for three years.

A security clearance issued for information and documents marked with the SECRET classification level shall be valid for five years.

A security clearance issued for information and documents marked with the CONFIDENTIAL classification level shall be valid for ten years.

A security clearance issued for information and documents marked with the RESTRICTED classification level shall be valid for fifteen years.

Extension of Security Clearance Validity
Article 75

The Council Office shall inform the security clearance holder in writing that he/she may submit an application for the extension of the security clearance validity, no later than six months before the clearance validity expiration.

In addition to submitting such an application for extending the personnel security clearance validity referred to in paragraph 1 of this Article, the applicant shall notify the Council Office of all changes of the information contained in the previously submitted security questionnaire along with the evidence, and the competent body referred to in Article 54 of this law shall carry out the security vetting again.

The provisions contained in Articles 48 to 63 and Article 66 of this law shall be applied to the procedure for the repeated security vetting referred to in paragraph 2 of this Article, unless otherwise provided by an international agreement.

Provisional Prohibition of Right of Access
Article 76

If any disciplinary procedure has been initiated against the person who has been issued a security clearance for a serious violation of official duty, military discipline or work duties and responsibilities, or against whom the criminal proceedings have been instituted due to the reasonable suspicion that such a person has committed a criminal offence, he/she shall be prosecuted *ex officio,* or in the event the misdemeanor proceedings have been initiated against the him/her for a misdemeanor envisaged by this law, the head of the public authority may temporarily prohibit, by means of decision, the access to classified information to the above person until the closure of the proceedings resulting in the enforceable ruling.

Clearance Checkout
Article 77

If it is established that the person who has been issued a personnel security clearance does not use or keep classified information in accordance with this law and other regulations, or that such a person does not meet the requirements for issuing a security clearance any more, the Council Office shall issue a decision to terminate the validity of security clearance validity before its expiration date or to restrict the right of access to classified information marked with a particular classification level.

The statement of reasons accompanying the decision 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 Council Office referred to in paragraph 1 of this Article shall be final and an administrative dispute may be initiated against it.

Issuance of Security Permit to Foreign Persons
Article 78

The Council Office shall issue a security permit to a foreign person in accordance with a concluded international agreement.

Upon receipt of an application, the Council Office shall check out, through the international exchange of information, whether the applicant has been issued a security clearance by the state authority of the country of his/her citizenship or of the country in which he/she has the seat or by an international organization he/she is a member of.

The security permit shall only be issued for access to information and documents defined in the international agreement the Republic of Serbia has concluded with a foreign country, an international organization or other international entity.

The provisions of this law governing the issuance of security clearance shall be applied accordingly to the issuance of security permit to a foreign person.

Official Records and Other Information Related to Security Clearances and Security Permits
Article 79

The Council Office shall keep unified central records on issued security clearances and security permits, decisions to issue security clearances and security permits, decisions to refuse issuance of security clearances and security permits, decisions to extend security clearance and security permits validity and decisions to restrict or terminate the validity of security clearances and security permits, as well as records on statements signed by the persons who have been issued security clearances or security permits.

The Council Office shall keep applications for issuing security clearances or security permits, security questionnaires and reports on security vettings with a recommendation.

Records on Security Vettings
Article 80

The body competent for the security vetting referred to in 54 of this law shall keep records on security vettings and keep documents on such vettings with a copy of the report and a recommendation.

The information contained in the security vetting may only be used for the purposes it has been collected for.

Application of Regulations on Personal Data Protection
Article 81

The person shall have the right to examine the data contained in the security clearance, as well as other rights based on such examination in accordance with the law governing the personal data protection, except for the examination of information which would reveal the methods and procedures used during the collection of information, as well as identify the sources of information contained in the security clearance.

Records on Public Authorities
Article 82

The public authority shall keep records on decisions to issue security clearances to persons who perform certain functions within the public authority or who are in its employ or perform services for it.

The decision to issue security clearances to persons referred to in paragraph 1 of this Article shall be kept in a special section of his/her personal file and the information contained in the decision may be used only in connection with the enforcement of the provisions of this law or the regulation adopted on the grounds of this law.

More Detailed Regulation on Content, Form and Method of Keeping Records
Article 83

The content, form and method of keeping records, as well as the period of safekeeping information referred to in Articles 79, 80 and 82 of this law, shall be prescribed by the Government at the proposal of the Council Office.

VI. CONTROL AND SUPERVISION

INTERNAL CONTROL

Article 84

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

A special work post for internal control and other technical operations concerning determination and protection of classified information shall be established within the work post classification at the ministries competent for internal affairs and defense affairs, the Security and Information Agency and other public authorities, where appropriate, or the existing organizational unit within the framework of the ministries or the agency shall be specifically engaged to perform these assignments and activities.

Objective of Internal Control
Article 85

The internal control shall provide regular monitoring and evaluation of particular 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 shall, either directly or through an authorized person, perform internal control by direct inspection, adequate checkouts and consideration of the submitted reports.

2. OFFICE OF THE COUNCIL ON NATIONAL SECURITY AND CLASSIFIED INFORMATION PROTECTION

Status of the Council Office
Article 86

The Council Office is a service of the Government having the capacity of the legal person whose remit comprises activities for the enforcement and control of the implementation of this law and supervision of the enforcement of this law.

Remit of the Council Office
Article 87

In accordance with this law, the Council Office shall:

1) act upon applications for issuing security clearances and security permits;
2) ensure the implementation of standards and regulations in the field of classified information protection;
3) take care of the implementation of the undertaken international obligations and international agreements concluded between the Republic of Serbia and other countries or international bodies and organizations in the field of classified information protection, and cooperate with the relevant authorities from foreign countries and bodies of international organizations;
4) develop and keep the Central Registry of Foreign Classified Information;
5) propose the form of security questionnaire;
6) propose the form of recommendation, security clearance and security permit;
7) keep records on issued security clearances or security permits, as well as records on refusals to issue such clearances or permits;

8) organize trainings for classified information users in accordance with the relevant standards and regulations;
9) propose to the Government a plan of classified information protection in case of contingencies and emergencies;
10) revoke the classification of information in accordance with the provisions of this law;
11) perform activities relating to the classified information protection after the public authorities have ceased to exist without a legal successor;
12) cooperate with the public authorities in the enforcement of this law;
13) perform other operations envisaged by this law and regulations adopted on the grounds of this law.

The Director of the Council Office shall submit to the Government an annual report on the activities performed within the remit of the Council Office.

Takeover of Classified Information
Article 88

The Council Office shall take over classified information of the public authority that has ceased to exist without a legal successor, or shall entrust another public authority with safekeeping and using of such information.

Director of the Council Office
Article 89

The Government shall appoint and release of duty the Director of the Office of the Council after obtaining an opinion from the National Security Council.

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

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

The person meeting the general requirements for employment by the state authorities, having a university degree and at least ten years of work experience in the field of security shall be appointed Director of the Council Office.

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

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

The Director of the Council Office shall be a civil servant holding a high-ranking position.

Termination of Duty
Article 90

The duty of the Director of the Office of Council shall be terminated for the reasons established by the law regulating the rights and obligations of civil servants.

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

Deputy Director of the Council Office
Article 91

The Council Office shall have the Deputy Director appointed by the Government at the proposal of the Director of the Office of the Council.

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

The person meeting the general requirements for employment by the state authorities, having a university degree and at least nine years of work experience in the field of classified information protection shall be appointed Deputy Director of the Council Office.

The Deputy Director may not be a member of any political party.

The Deputy Director of the Council Office shall be a civil servant holding a high-ranking position.

The Deputy Director shall perform the function of the Director of the Office of the Council in case of his/her absence, death, expiration of term of office, release from duty and temporary or permanent inability to discharge the function.

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

Document on the Internal Organization and
Classification of Work Posts and Salary Rise
Article 92

The Director of the Council Office shall adopt a document on internal organization and work post classification to be approved by the Government upon obtaining an opinion from the National Security Council.

The person working on the classified information protection may be employed by the Council Office if he/she has undergone a special security vetting.

The regulations concerning the employment relations of civil servants and associate officers shall be applied to the employment relations of the Director of the Council Office, the Deputy Director of the Council Office and the employees of the Council Office working on the classified information protection.

Due to the special working conditions, complexity and nature of the activities, the Director of the Council Office, the Deputy Director of the Council Office and the employees of the Council Office working on the protection of classified information, may receive a salary rise of up to 20% a month in relation to the salary of other civil servants and associate officers whose work posts are classified in the same group or rank, as well as to the work posts of civil servants and associate officers who work on the protection of classified information, pursuant to the by-law of the Government.

Obligations of the Council Office Relating to Foreign Classified Information
Article 93

The exchange of classified information with foreign countries and international organizations shall be carried out through the Council Office, unless otherwise prescribed by a specific law or a concluded international agreement.

Central Registry of Foreign Classified Information
Article 94

The Council Office shall establish, keep and secure the Central Registry of Foreign Classified Information and Documents.

The public authority, which has received foreign classified information and document in accordance with a specific law or a concluded international agreement the Republic of Serbia has concluded with a foreign country, an international organization or other international entity, shall establish, keep and secure a separate registry of foreign classified information.

The report containing numerical indicators of the exchange of classified information with a foreign country or an international organization shall be submitted by the public authority to the Council Office of the Council at least once a year.

Sending and Receiving Notifications
Article 95

The Office of the Council shall send a notification to a foreign country or an international organization relating to the security of foreign classified information provided within the international exchange.

The Council Office of the Council shall receive notifications from the foreign country or an international organization relating to the security of classified information that the Republic of Serbia has provided in the international exchange.

Exchange of Information without a Concluded International Agreement
Article 96

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

3. Supervision

Article 97

The Ministry competent for the judiciary (hereinafter: the Ministry) shall conduct the supervision of the enforcement of this law and regulations adopted on the grounds of this law.

Pursuant to this law, when conducting such supervision, the Ministry shall:

1) monitor the situation in the field of classified information protection;
2) draft regulations necessary for the enforcement of this law;
3) give its opinion on draft regulations in the field of classified information protection;
4) propose to the Government the content, form and method of keeping records on classified information, as well as regulations governing the form of security questionnaire or the form of recommendation, security clearance and security permit;

5) orders implementation of measures for the improvement of classified information protection;
6) control application of criteria for designating the classification level, and perform other control activities in accordance with the provisions of this law;
7) file criminal charges, applications instituting misdemeanor proceedings, and propose initiating another procedure due to the violation of the provisions of this law and pursuant to law;
8) cooperate with the public authorities in the enforcement of this law within its remit;
9) perform other activities envisaged by this law and regulations adopted on the grounds of this law.

The minister competent for the judiciary shall submit to the National Assembly Committee competent for the supervision and control in the field of defense and security an annual report on the activities performed in the enforcement and implementation of this law.

When conducting the supervision the Ministry shall carry out the control of the implementation of measures relating to security, use, exchange and other classified information processing operations without previously notifying the public authority, authorized person, security officer or the classified information user of such control.

The Ministry shall perform the activities referred to in paragraph 1, 2 and 4 of this Article through the authorized persons who have undergone a special security vetting.

The authorized persons referred to in paragraph 5 of this Article shall conduct the supervision by applying regulations on inspectoral supervision.

The authorized persons referred to in paragraph 5 shall be entitled to an official identity card.

Due to the specific working conditions, complexity and nature of the activities, the authorized persons referred to in paragraph 5 of this Article may receive a salary rise of up to 20% a month in relation to the salary of other civil servants and associate officers at the Ministry competent for the judiciary who work on the supervision of judicial bodies, pursuant to the document of the Government.

A more detailed regulation on the official identity card and working method of the authorized persons shall be adopted by the minister competent for the judiciary.

VII. PENAL PROVISIONS

Criminal Offence
Article 98

Anyone who communicates, submits or makes available without authorization to an incompetent person the information or documents entrusted to him/her or the information or documents obtained in another manner or anyone who procures information or documents that constitute classified information marked with the RESTRICTED or CONFIDENTIAL classification level, as defined by this law, shall be punished with a prison sentence ranging from three months to three years.

If the offence referred to in paragraph 1 of this Article has been committed in relation to information marked with the SECRET classification level, pursuant to this law, the perpetrator shall be punished with a prison sentence ranging from six months to five years.

If the offence referred to in paragraph 1 of this Article has been committed in relation to information marked with the TOP SECRET classification level, pursuant to this law, the perpetrator shall be punished with a prison sentence ranging from one to ten year.

If the offence referred to in paragraphs 1 to 3 of this Article has been committed for gain or in order to release or use classified information abroad, or if it has been committed during wartime or the state of emergency, the perpetrator shall be punished for the offence referred to in paragraph 1 of this Article with a prison sentence ranging from six months to five years, and for the offence referred to in paragraph 2 of this Article to a prison sentence ranging from one to eight years and for the offence referred to in paragraph 3 of this Article with a prison sentence ranging from five to fifteen years.

If the offence referred to in paragraphs 1 to 3 of this Article has been committed out of negligence, the perpetrator shall be punished for the offence referred to in paragraph 1 of this Article with a prison sentence of up to two years, and for the offence referred to in paragraph 2 of this Article with a prison sentence ranging from three months to three years and for the offence referred to in paragraph 3 of this Article with a prison sentence ranging from six months to five years.

Misdemeanor Liability of the Person in Charge within the Public Authority
Article 99

The person in charge within the public authority shall be fined in the amount from RSD 5,000 to 50,000 if:

1) he/she designates as classified information and document that evidently do not refer to protected interests (Article 8, paragraph 2);
2) he/she transfers the authorization for the determination of classified information to a third party (Article 9, paragraph 3);
3) he/she designates classified information contained in the document with an inadequate level of classification (Article 11, paragraph 2);
4) he/she issues a decision to determine information to be classified without the statement of reasons (Article 11, paragraph 4);
5) he/she does not revoke the classification of information upon the occurrence of the date of event after which the classification of information shall terminate (Articles 17 and 18);
6) he/she does not revoke the classification of information after the expiration of the statutory time limit for the termination of classification of information (Article 19);
7) he/she does not conduct a periodical assessment of information classification (Article 22);
8) he/she does not revoke the classification of information on the grounds of the decision of the Commissioner for Information of Public Importance and Personal Data Protection or the decision of the competent court (Article 25);
9) he/she changes the document classification contrary to the provisions of Article 27 of this law;
10) he/she fails to inform the public authorities of the change in classification level and revocation of classification (Article 28);
11) he/she does not prescribe, arrange and supervise the implementation of the general and special measures for the protection of classified information which are appropriate for its classification level (Articles 32 and 33);
12) he/she does not to present a statement to be signed by the person issued a clearance for access to classified information confirming that such a person has been briefed on the regulations governing the protection of classified information (Article 42, paragraph 3);
13) he/she provides classified information to legal and natural persons contrary to the provision of Article 46 of this law;

14) he/she does not keep records on decisions to issue personnel security clearances for access to classified information (Article 82, paragraph 1);
15) he/she does not keep a decision to access classified information in a separate section of the personal file (Article 82, paragraph 2);
16) he/she does not organize an internal control of the classified information protection (Article 84, paragraph 1);
17) he/she does not take measures to establish, keep and secure the special registry of foreign classified information (Article 94, paragraph 2);

Misdemeanor Liability of Security Officer
Article 100

A security officer who fails to take measures for the protection of classified information shall be fined for misdemeanor in the amount ranging from RSD 5,000 to 50,000 (Article 34).

VIII. TRANSITIONAL AND FINAL PROVISIONS

Article 101

The Office of the Council on National Security, established in accordance with Article 8 of the Law on the Foundations of the Organization of Security Services in the Republic of Serbia (The Official Gazette of RS, No. 116/07), shall continue to perform its activities under the name of the Office of the Council on National Security and Classified Information Protection on the date of entry into force of this law.

The Director of the Office of the National Security Council, who has been appointed pursuant to the law referred to in paragraph 1 of this Article shall continue to discharge the function of Director of the Office of the Council on National Security and Classified Information Protection until the expiration of the period he/she has been appointed for.

Appointment of Deputy Director
Article 102

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

Adoption of Document on the Internal Organization and Work Post Classification and Transfer of Employees
Article 103

The document on internal organization and work post classification within the Council Office shall be adopted within sixty days from the date of entry into force of this law.

The required number of employees shall be taken over from other public authorities that perform activities in the field of classified information protection by the Council Office within ninety days from the date of adopting the document referred to in paragraph 1 of this Article.

Passage of By-laws
Article 104

The by-laws envisaged by this law to be passed by the Government shall be passed within the period of six months from the date of entry into force of this law.

The by-laws prescribed by this law to be passed by other public authorities shall be passed within the period of one year from the date of entry into force of this law.

Until the passage of the by-laws referred to in paragraphs 1 and 2 of this Article, the provisions of the valid by-laws, which are not contrary to the provisions of this law, shall apply.

Review of Existing Classification Designations
Article 105

From the date of entry into force of this law, information and documents that have been designated with a classification level on the basis of the previously passed regulations shall retain the type and level of classification designated under the earlier regulations.

The heads of the public authorities shall review the designations of information referred to in paragraph 1 within two years from the date of entry into force of this law in accordance with the provisions of this law.

Harmonization of By-laws and Issuance of
Security Clearances to Employees of Public Authorities
Article 106

The public authorities shall be obliged to harmonize their organization with the provisions of this law within the period of one year from the date of entry into force of this law.

The public authorities shall be obliged to ensure, within two years from the date of entry into force of this law, that all employees, who must have access to classified information due to their work duties or functions, are issued personnel security clearances for access to classified information, pursuant to this law.

Harmonization of International Agreements
Article 107

Within two years from the date of entry into force of this law, the competent authorities of the Republic of Serbia shall review the provisions of the existing international agreements the Republic of Serbia has concluded in the field of the classified information protection, and shall initiate the procedure for amending such international agreements, where appropriate.

Application of Valid Laws in the Part Relating to Determination and
Protection of Classified Information
Article 108

The provisions of the valid laws regulating the activities of the public authorities in the part relating to the determination and protection of classified information and foreign classified information, which are not contrary to the provisions of this law, shall apply until the date of commencement of the application of this law.

Expiration of Validity of Laws and Other Regulations
Article 109

As of the date of commencement of the application of this law, the validity of the following shall be terminated:

1) Article 123 of the Law on Defense (the Official Gazette of RS, No. 116/07);

2) provisions of Chapter VI - Security and Protection Measures referred to in Articles 67 to 86 of the Law on Defense (the Official Gazette of RS, Nos. 43/94, 11/95, 28/96, 44/99 and 3/02 and the Official Gazette of RS, No. 116/07);
3) Article 45, paragraph 2 of the Law on Personal Data Protection (the Official Gazette of RS, No. 97/08).

Entry into Force
Article 110

This law shall enter into force on the eighth day after its publication in the Official Gazette of the Republic of Serbia and shall apply as of 1 January 2010.