LAW FOR THE PROTECTION OF THE CLASSIFIED INFORMATION

Prom. SG. 45/30 Apr 2002, corr. SG. 5/17 Jan 2003, amend. SG. 31/4 Apr 2003, amend. SG. 52/18 Jun 2004, suppl. SG. 55/25 Jun 2004, suppl. SG. 89/12 Oct 2004

Chapter one. GENERAL PROVISIONS

Art. 1. (1) This law shall provide the public relations, connected with the creating, the processing and the preservation of classified information, as well as the conditions and the order for conceding of access to it.

(2) Objective of the law is the protection of the classified information of non regulated access.

(3) Classified information in the context of this law shall be the information, constituting state or service secret, as well as the foreign classified information.

Art. 2. This law shall also be applied with regard to the foreign classified information, conceded by other country or international organisation, as far as other international agreement, entered into force, to which the Republic of Bulgaria is a party, does not provide other.

Art. 3.(1) Access to classified information shall be conceded only to persons, who have received permission for access, observing the principle "necessary to be known" except this law provides other.

(2) The principle "necessary to be known" shall consist in restricting the access to only determined classified information and only for persons, which official obligations or concrete assigned task impose such access.

Chapter two. BODIES FOR PROTECTION OF THE CLASSIFIED INFORMATION

Section I. State commission for the security of the information

Art. 4.(1) The State commission for the security of the information (SCSI) shall be a state body, which shall implement the policy of the Republic of Bulgaria for protection of the classified information.

(2) The State commission for the security of the information shall be primary administrator with budget resources.

Art. 5. The State commission for the security of the information shall be supported by administration, which activities, structure and organisation of the work shall be determined with a structural regulation, approved by the Council of Ministers.

Art. 6.(1) The State commission for the security of the information shall be a collegial body and it shall be consisted by five members, including a chairmen, and deputy which shall be determined with a decision of the Council of Ministers for a term of 5 years upon a proposal by the Prime Minister.

(2) members of the commission can only be persons with higher education.

Art. 7.(1) The chairman of the SCSI shall present annual report to the Council of Ministers about the overall activity for the status of the protection of the classified information.

(2) The Council of Ministers shall present the report of para 1 to the National Assembly, which shall be approved with a decision.

(3) The chairman of SCSI shall present information equal in extent and content about the activity of the commission to the chairman of the National Assembly of the Republic of Bulgaria and to the Prime Minister.

Art. 8. The State commission for the security of information shall:

1. organise, implement, co-ordinate and control the activity for protection of the classified information;

2. ensure the equal protection of the classified information;

3. implement its activity in close co-operation with the Ministry of Defence, the Ministry of Interior, the Ministry of Foreign Affairs and the services for security and public order.

Art. 9. The SCSI in implementing its activity shall:

1. determine directions and approve action plans for the organisational units in case of occurring of danger of infringing of state interests due to unregulated access to classified information;

2. implement analysis and assessment of the readiness for the protection of the classified information in case of occurring of danger of infringement of the interests, protected by law, due to unregulated access to classified information and give obligatory instruction in this sphere;

3. organise and conduct preventive activity for prevention and reduction of the harmful consequences from unregulated access to classified information;

4. develop and submit for approval to the Council of Ministers drafts of normative acts in the field of protection of the classified information;

5. organise and ensure the functioning of the registries in the field of the international relations;

6. organise, control and be responsible for the fulfilment of the obligations for protection of the classified information, contained in international agreements, to which the Republic of Bulgaria is a party;

7. implement general management of the activity for the investigations about

reliability of the persons, who are necessary to work with classified information and about the issuing of permission to access to the respective level of classified information, called hereinafter "permission";

8. implement general management of the activity for investigation of individuals and corporate bodies, applying for the concluding of contract or implementing contract, connected with access to classified information, and approve model of certificate for security according to this law, called hereinafter "certificate";

9. implement investigation together with the services for security and upon their proposal issue permission for the persons, proposed for appointment as officials for the security of information;

10. issue certificates, confirming before the foreign authorities, that Bulgarian individuals or corporate bodies have permission, respectively certificate;

11. implement together with the security services investigation of Bulgarian citizens, who apply for taking a position or fulfilment of concrete assigned tasks, imposing work with classified information of another state or international organisation after receiving of written request by the competent body for security of the information of the respective state or international organisation;

12. keep unified registers of the issued. the withdrawn or the terminated permissions, certificates and confirmations, of the refusals for issuing or the termination of such, as well as register of the materials and the documents, containing classified information, constituting state or official secret;

13. inform immediately the Prime Minister in case of unregulated access to classified information with level of classifying "Top secret";

14. organise and co-ordinate the training for work with classified information;

15. implement methodical guidance for the officials for the security of information;

16. implement general control for the protection of classified information, preserved, processed and submitted to automated information systems or networks;

17. give permission for visit of persons for implementing inspections, conducted by force of international agreements for mutual protection of the classified information.

Art. 10.(1) In implementation of its tasks under art. 9 the SCSI shall:

1. be able to require information from the information massifs of the services for security and public order;

2. receive immediately and free of charge the necessary information from the state bodies and the bodies of the local government;

3. receive immediately and free of charge the necessary information from the individuals and the corporate bodies according to the laws in effect. The persons can refuse to concede information, which is not connected wit the investigation about reliability, about which they have given consent or have been notified by the respective order;

4. issue obligatory instructions to the subjects, obliged under the law.

(2) The conditions and the order for conceding the information of para 1, items 1, 2 and 3 shall be provided in the regulation for implementation of the law.

Section II. Functions of the services for security

Art. 11.(1) The services for security shall:

1. implement the investigations for reliability of their employees and of the candidates for employment, issue, terminate and withdraw the permissions of these persons;

2. implement investigation of individuals and corporate bodies, who apply for concluding or who fulfil a contract, connected with access to classified information and issue certificates for compliance with the requirements for security according to this law;

3. co-operate for the fulfilment of the tasks of SCSI under art. 9, items 9, 10, 11, 13, 14 and 17;

4. co-operate for the fulfilment of the tasks of para 2, item 3 and of art. 12, item 2.

(2) The National service "Security" of the Ministry of Interior, apart from the functions of para 1 shall:

1. implement the investigations for reliability of the persons, to whom is necessary to work with classified information and issue, terminate, withdraw or refuse permission for access to the respective level of classification, except in the cases of art. 22, para 1, item 5;

2. issue a confirmation to foreign individuals and corporate bodies on the basis of already issued permission or certificate by the respective corporate body of another state or international organisation and after implemented investigation in the Republic of Bulgaria, called hereinafter "confirmation", except the cases of para 3, item 3;

3. implement direct control for the protection of the classified information and for the observing of the legal provisions in this sphere.

(3) In the structures of then Ministry of defence and of the Bulgarian Army, except service "Military information", apart from the functions of para 1 and para 2, item 3 service "Security – military police and military counter - intelligence" shall:

1. implement investigations, issue, terminate and withdraw permissions of Bulgarian citizens – conscripts, military servicemen at regular military service, at conscript military service, from the reserve and civil persons with official or employment legal relation in the structures of the Ministry of Defence and the Bulgarian Army, as well as in the secondary administrators with budget credits at the Minister of Defence;

2. implement investigations, issue, terminate and withdraw permissions of individuals, respectively certificates of corporate bodies, applying for or implementing activity for the Ministry of Defence and the and the Bulgarian Army and in the secondary administrators with budget credits at the Minister of Defence;

3. issue confirmations to foreign citizens for work and/or training in the Ministry of Defence and in the Bulgarian Army, as well as in the secondary administrators with budget credits at the Minister of Defence.

(4) In implementation of the tasks of para 1, 2 and 3 the services for security shall have right:

1. to apply and use intelligence intelligence methods under conditions and by order, determined with a law.

2. to apply and use special intelligence means under the Law for the special intelligence means for persons, applying for receiving of access to information with level of classification for security "Top secret";

3. to use data from their information massifs about individuals and corporate bodies – subject to investigation;

4. to preserve the data, received in the process of investigation of the individuals and of candidates – individuals and corporate bodies, at concluding of fulfilment of a contract, connected with access to classified information;

5. to preserve data about unregulated access to classified information;

6. to receive the necessary information from the state bodies, the bodies of the local government, the individuals and the corporate bodies, according to the laws in effect. The conditions and the order for conceding of the information shall be regulated with the regulation for implementation of the law.

(5) In implementation of the tasks of para 1 – 4 the services for security shall interact between themselves.

Art. 12. For implementing of direct control for protection of the classified information and for observing of the legal provisions in this field the chiefs of the National service "Security" and service "Security – military police and military counter - intelligence" shall with a written order determine employees, who shall have right:

1. to access to the sites and the premises in the organisational unit – subject to control, including for making inspection of these sites and premises;

2. to access to the documents, connected with the organisation for protection of the classified information in the organisational unit – subject to the control;

3. to access to the automated information systems or networks for creating, preservation, processing and transfer of classified information with objective to be established the reliability of the protection;

4. if necessary to require written and verbal explanations from the chiefs and the employees of the organisational unit – subject to control.

5. to receive information from other organisational units and to require explanations if necessary from their chiefs and employees about the activity for creating, processing, preservation and conceding of the classified information in connection with implemented check in the organisational unit – subject to control;

6. to attract experts when specialised knowledge is necessary for clarifying circumstances, connected with an implemented check;

7. to give concrete prescriptions in connection with the protection of the classified information.

Art. 13. The order for implementing of the checks of art. 12 shall be determined with an ordinance, approved by the Council of Ministers.

Art. 14. Directorate "Protection of the means for communication" of the Ministry of Interior shall:

1. implement the activities for cryptographic protection of the classified information according to art. 124 of the Law for the Ministry of Interior;

2. issue certificate for security of the automated information systems or networks, used for work with classified information;

3. co-ordinate and control the activity for protection from parasitic electric –magnetic emissions of the technical means, processing, preserving and transferring classified information;

4. implement and control the training for work with cryptographic methods and means of the persons, received permission for access to classified information.

Section III. Services for public order

Art. 15. The services for public order shall implement investigations for the reliability of their employees and of the candidates for work, issue, terminate and withdraw the permissions of these persons.

Art. 16.(1) In implementation of the tasks of art. 15 the services for public order shall have right:

1. to apply and use operational – investigation methods under conditions and by order, determined with a law;

2. to use data from their information massifs about individuals and corporate bodies – subject to investigation;

3. to preserve the data, received in the process of investigation of its employees;

4. to preserve data about cases of unregulated access to classified information by the employees of art. 15;

5. to receive any necessary information from other organisational units in connection with the investigations of the persons of art. 15.

(2) The services for public order shall, within the limits of their functions and authorities, be obliged to render co-operation to the services for security in connection with the fulfilment of their tasks under art. 11.

Section IV. Obligations of the organisational units

Art. 17. The organisational units shall:

1. apply the requirements for protection of the classified information and control their observing;

2. be responsible for the protection of information;

3. in case of unregulated access to classified information inform immediately SCSI and undertake measures for restricting of the unfavourable consequences;

4. concede information under art. 10, para 1, item 2, art. 11, para 4, item 6 and art. 16, para 1, item 5.

Art. 18.(1) The employees of the organisational units, received permission for access to the corresponding level of classified information, shall be obliged:

1. to protect the classified information from unregulated access;

2. to inform immediately the employee for security of the information about cases of unregulated access to classified information;

3. to inform the employee for security of the information about all cases of changes of the classified materials and documents, for which there is no unregulated access;

4. to pass periodic health examinations at least once in two years and psychological examinations under the conditions and by the order of art. 42, para 3.

(2) Each person, who have received permission to access to classified information with level of classification "Top secret" shall be obliged to inform in writing the employee for security of information about each private travel abroad before the date of departure, except

when the travel is in states with which the Republic of Bulgaria has concluded agreements for mutual protection of classified information.

(3) Para 2 shall not be applied with regard to the persons of art. 39, para 1.

(4) The employees of the services for security and for public order shall notify in writing their chiefs about each travel abroad.

(5) The military servicemen and then civil persons of the Ministry of Defence and the Bulgarian Army shall inform in writing the chief of service "Security – military police and military counter - intelligence" about each travel abroad.

Art. 19. The persons, who have received permission for access to classified information in connection with the fulfilment of concrete assigned task shall be obliged to observe the conditions and the order for protection of the classified information.

Section V. Employees for the security of the information

Art. 20.(1) The chief of the organisational unit shall manage, organise and control the activity for protection of the classified information.

(2) The chief of the organisational unit shall appoint an employee for the security of the information after receiving of permission to access to classified information, issued by SCSI.

(3) As exception, depending on the level and the amount of the classified information the chief of the organisational unit can fulfil the functions of employee for the security of the information if he meets the requirements of art. 21.

(4) The employee for the security of the information shall be directly subordinated to the chief of the organisational unit.

Art. 21.(1) As employee for the security of the information can be appointed a person, who meets the following requirements:

1. to have Bulgarian citizenship;

2. to have received permission for access to the respective level of classified information under the conditions and by the order of chapter five.

(2) After the appointment the employee for the security of the information shall obligatory pass training in the field of the protection of the classified information.

Art. 22.(1) The employee for the security of the information shall:

1. follow about the observing of the requirements of this law and of the international agreements in connection with the protection of the classified information;

2. apply the rules for protection of the classified information;

3. develop plan for protection of the organisational unit with physical and technical means and follow its fulfilment;

4. implement periodic checks of the accounting and the movement of the materials and the documents;

5. implement simple investigation under art. 47;

6. implement the procedure for simple investigation within the organisational unit and

keep register of the investigated persons;

7. notify SCSI upon the elapse of the term of the permissions, at leaving or discharge of the employee, as well as at necessity of change of the permission, connected with the access to certain level of classification;

8. inform immediately in writing the SCSI and the competent service about each change, referring to the circumstances, connected with the issued permissions, authorisations, certificates or confirmations;

9. keep account of the cases of unregulated access to classified information and of the undertaken measures, about which informs the SCSI immediately;

10. follow the correct determining of the level of classification of the information;

11. develop plan for protection of the classified information in case of war, military or other state of emergency;

12. organise and conduct the training of the employees in the organisational unit in the field of protection of the classified information.

(2) If the circumstances of para 1, items 7, 8 and 9 exist the employees for the security of the information in the services for security of the information and public order shall inform immediately the chiefs of the services.

(3) The employees for the security of the information in the Ministry of Defence and in the Bulgarian Army shall, if the circumstances of para 1, items 8 and 9 exist, inform immediately service "Security – military police and military counter - intelligence".

Section VI. Administrative units for the security of the information

Art. 23. For fulfilment of the tasks of art. 22 and depending on the amount of the classified information the employee for the security of the information can be assisted by the administrative units for the security.

Art. 24. As employees in the units of art. 23 shall be appointed persons, who meet the requirements of art. 21.

Chapter three. KINDS OF CLASSIFIED INFORMATION AND LEVELS OF CLASSIFICATION

Section I. Classified information

Art. 25. State secret shall be the information, determined in the list of appendix No 1, the unregulated access to which would create danger or would damage the interests of the Republic of Bulgaria, connected with the national security, the defence, the foreign policy or the protection of the constitutionally established order.

Art. 26.(1) Official secret shall be the information, created or preserved by the state bodies or the bodies of the local government, which is not state secret, the unregulated access

to which would influence unfavourably the interests of the state or would hamper other legally protected interest.

(2) The information, subject to classification as official secret, shall be determined with a law.

(3) The chief of the respective organisational unit shall, within the framework of the law, announce a list of the categories of information of para 2 for the sphere of activity of the organisational unit. The order and the way for announcing of the list shall be determined in the regulation for implementation of the law.

Art. 27. Foreign classified information shall be the classified information, conceded by another state or international organisation by force of international agreement, to which the Republic of Bulgaria is a party.

Section II. Levels of classification for security of the information

Art 28. (1) The levels of classification for security of the information and their secrecy grading shall be:

1. "Top secret";
2. "Secret";
3. "Confidential";
4. "For official use".

(2) The information, classified as state secret, shall be marked with secrecy grading:

1. "Top secret" – in the cases, when unregulated access would endanger in exclusively high degree the sovereignty, the independence or the territorial entity of the Republic of Bulgaria or its foreign policy and international relations, connected with national security, or would be able to create danger from occurrence of irrecoverable or exclusively big damages, or to cause such damages in the field of national security, the defence, the foreign policy or the protection of the constitutionally established order;
2. "Secret" – in the cases, when unregulated access would endanger in high degree the sovereignty, the independence or the territorial entity of the Republic of Bulgaria or its foreign policy and international relations, connected with national security, or would be able to create danger from occurrence of difficult to recover or big damages, or to cause such damages in the field of national security, the defence, the foreign policy or the protection of the constitutionally established order;
3. "Confidential" – in the cases, when unregulated access would endanger the sovereignty, the independence or the territorial entity of the Republic of Bulgaria or its foreign policy and international relations, connected with national security, or would be able to create danger from occurrence of damages, or to cause such damages in the field of national security, the defence, the foreign policy or the protection of the constitutionally established order.

(3) The information, classified as official secret, shall be marked with secrecy grading "For official use".

(4) With objective to ensure additional protection, when this is imposed by the character of the information or when it is provided in international agreements, to which e Republic of Bulgaria is a party, the SCSI shall, upon proposal of the Minister of Interior, the Minister of Defence or the directors of the services for security, be able to determine with a

decision:

1. additional marking of materials and documents with higher level of classification from "Top secret";

2. special order for creating, using, reproduction, conceding and preservation of these materials and documents;

3. the circle of the persons with right to access to these materials and documents.

Art. 29. The equalling of the levels of classification for security of the received foreign classified information or of the such information, conceded by the Republic of Bulgaria to another state or international organisation in implementation of an international agreement for the Republic of Bulgaria and for the respective foreign state or international organisation, entered into force, shall be implemented in compliance with the provisions of the contract.

Chapter four. MARKING OF THE INFORMATION

Section I. Procedure for marking of the classified information

Art. 30.(1) The marking of the classified information shall be implemented by putting of respective secrecy grading.

(2) The secrecy grading shall contain:

1. level of classification;

2. date of classification;

3. date of expiry of the term of classification, when it is different from the date of expiry of the terms of art. 34, para 1;

4. the legal ground for classification.

(3) A collection of materials and/or documents, containing classified information with different secrecy grading, shall receive secrecy grading, corresponding to the highest level of classification of material or document in this collection.

Art. 31.(1) The secrecy grading shall be determined by the person, who has the right to sign the document, containing classified information or certifying the existence of classified information in a material, different from this document.

(2) The person, who has created the document or the material, containing classified information, in case he is different from the person of para 1, shall be obliged to put secrecy grading, valid till its final determining by the person of para 1.

(3) The persons. obliged to mark the classified information, are responsible for putting or not of secrecy grading.

(4) The putting, the change or the deleting of secrecy grading shall be implemented only within the framework of the access, conceded to the person to classified information.

(5) No marking with secrecy grading shall be admitted, not complying with the level of classification, determined by the order of this law and the regulation for its implementation.

(6) Without the consent of the person of para 1 or of his higher chief the level of classification cannot be changed or deleted.

(7) Ungrounded change of the level of classification shall not be admitted;

(8) When a person, who has received by the lawfully established order classified information, finds, that the level of the classification is incorrectly defined, he shall immediately inform about this the person of para 1 or his higher chief.

(9) In case of change of the level of classification the notified person shall be obliged immediately to announce this to the recipient. At submitting of the classified information to third persons, the recipient shall immediately notify these persons about the change.

(10) The chiefs of the organisational units shall organise the training of the employees, subordinated to them about the conditions and the order for marking of the information (the putting, the change and the deleting of the secrecy grading) under the methodical guidance of SCSI.

Art. 32 The order and the way of marking of the information shall be determined with the regulation for implementation of the law.

Section II. Preservation of the classified information

Art. 33.(3) The classified information shall be created, processed, conceded, preserved and destroyed under the conditions and by the order of this law and the by-law acts for its implementation, as well as in compliance with the provided kinds of protection, corresponding to the level of classification, except in an international agreement, to which the Republic of Bulgaria is a party, is provided other.

(2) In one year term after the elapse of the term for protection the information shall be conceded to the State archive fund unless a special law does not provide other.

(3) Destroying of information shall be admitted only after the elapse of one year after the term for its protection.

(4) The state commission for the security of the information shall permit the destroying of information after a proposal by a commission, formed with an order by the chief of the corresponding organisational unit. The commission shall:

1. give proposal which information does not have historic, practical or reference importance;

2. make proposal for destroying of documents and materials.

(5) The decision of SCSI for destroying of information shall be subject to court appeal before the Supreme Administrative Court.

Section III. Terms for protection of the classified information

Art. 34.(1) The following terms shall be determined for protection of the classified information, assumed from the date of creating it:

1. for information, marked with secrecy grading "Top secret" – 30 years;

2. for information, marked with secrecy grading "Secret" – 15 years;

3. for information, marked with secrecy grading "Confidential" – 5 years;

4. for information, classified as official secret – 2 years.

(2) With decision of SCSI, when the national interests impose this, the terms of para 1

can be extended, but with not more, than the initially defined.

(3) After the elapse of the terms para 1 and 2 the level of classification shall be removed and the access to this information shall be implemented by the order of the Law for access to public information.

(4) In the cases of full liquidation of the organisational unit, when a special law does not provide other, the information, classified as state or official secret, as well as all authorities for change of the level of classification, shall be conceded to SCSI.

(5) The terms of para 1 and 2 shall be applied also with regard to foreign classified information, except an international agreement, to which the Republic of Bulgaria is a party, provides other term.

Art. 35.(1) The State commission for the security of the information shall keep a register of the materials and the documents, containing classified information, being state or official secret.

(2) The register of para 1 shall contain data about:

1. the organisational unit, where is created the respective material or document;

2. the date of its creating and the date, provided for removal of the level of classification;

3. the identification number of the material or the document, under which it is kept in the register of para 1;

4. the legal grounds for classification of the material or the document and the secrecy grading;

5. change or removal of the level of classification and the date of implementing them.

(3) The chiefs of the organisational unit shall concede to SCSI the information of para 2, items 1, 2, 4 and 5 for entering in the register after the creating of the material or the document, containing classified information, being state or civil secret, respectively after removal or change of the level of classification.

(4) The persons of art. 31, para 1 shall reconsider regularly, at least once in two years, the terms for protection of each material or document, marked with secrecy grading, the existing of legal grounds for change or removal of the level of classification. At change of the level of classification shall be accounted for the term passed till the change of art. 34, para 1.

(5) The order for conceding of data for entering in the register, as well as the conditions and the order for implementing of references from the register shall be determined in the regulation for implementation of the law.

Chapter five. CONDITIONS AND ORDER FOR RECEIVING ACCESS TO CLASSIFIED INFORMATION

Section I. Conditions for receiving access to classified information

Art. 36. Nobody shall have right to access to classified information only by force of his official position, except the cases of art. 39.

Art. 37.(1) The chiefs of the organisational units, except the cases of para 2, shall

determine a list of the positions or the tasks, for which is required access to the respective level of classified information, constituting state secret.

(2) The chiefs of the services for security and public order shall determine the list of para 1 for these services.

Art. 38.(1) Access to classified information in connection with fulfilment of official obligations or concrete assigned tasks shall be permitted after:

1. implementing of investigation of the person for reliability;

2. conducting of training of the person in the field of protection of the classified information.

(2) No investigation of the person for reliability shall be implemented in connection with the access to information, classified as official secret.

Art. 39.(1) No investigation for reliability shall be implemented with regard to:

1. the chairman of the National Assembly;

2. the President of the Republic of Bulgaria;

3. the Prime Minister;

4. the Ministers;

5. the chief secretary of the Council of Ministers;

6. the Members of the Parliament;

7. (suppl. SG 55/04) the judges of the Constitutional Court, the judges, the prosecutors, the attorneys and the investigators.

(2) The persons of para 1, items 1, 2 and 3, assumed from the moment of taking the position, shall receive by right access to all levels of classified information for the term of taking their position.

(3) The persons of para 1, items 4, 5, 6 and 7 shall receive, assumed from the moment of taking the position, by right access to all levels of classified information for the term of taking their position, observing the principle "necessary to be known", when the information is:

1. for the ministries and the chief secretary of the Council of Ministers – within the circle of their competence;

2. for the Members of the Parliament – upon taken by the established order decision by a Parliamentary Commission or when a commission or the National Assembly have a closed session;

3. (suppl. SG 55/04) for the judges, the prosecutors, the attorneys and the investigators – only for concrete case.

Art. 39a. (new – SG 89/04) (1) Investigation for reliability shall not be implemented at or in connection with implementing their constitutional right to defense.

(2) The persons of para 1 shall receive by right access to all levels of classified information for the time, necessary for exercising their right to defense and observing the principle "need to be known".

Art. 40.(1) Permission for access to classified information, out of the cases of art. 39, shall be issued to a person, who meets the following requirements:

1. have Bulgarian citizenship, except the cases of chapter six, section VI;

2. is mature;

3. has graduated secondary education;

4. has not been convicted for premeditated crime of general character, regardless of the rehabilitation;

5. there is no pre-court or court procedure, started against the person for premeditated crime of general character;

6. is reliable from point of view of the security;

7. is not suffering from psychic diseases, certified by the respective order;

8. is determined as reliable for protection of secret.

(2) If there is international agreement, to which the Republic of Bulgaria is a party, or under the conditions of mutuality the requirements of para 1 shall not be applied with regard to citizens of other states, which implement in the Republic of Bulgaria tasks, assigned to them by the respective state or international organisation, in case they have permissions, issued by the respective competent body for security of the information of the other state or international organisation.

Art. 41. Reliability of the person from point of view of the security shall exist, when there are no data about:

1. implementing of activity against the interests of the Republic of Bulgaria or against interests, which the Republic of Bulgaria has obliged itself to protect by force of international agreements;

2. participation or implication in spy, terrorist, sabotage or diversion activity;

3. implementing of other activity against the national security, the territorial entity or the sovereignty of the country or aiming forceful change of the constitutionally established order;

4. implementing of activity, directed against the public order.

Art. 42.(1) Reliability of the person from point of view of protection of the secret exists, when there are no data about:

1. hiding or giving of incorrect information by the investigated person for the objectives of the investigation;

2. facts and circumstances, which would have given opportunity for blackmail of the investigated person;

3. inconsistency between the living standard of the investigated person and his incomes;

4. psychic disease or other disturbances of the psychic activity, which would influenced negatively the abilities of the investigated person to work with classified information;

5. dependence of the investigated person on alcohol and narcotic substance.

(2) For establishing the facts of para 1, items 4 and 5, the body, implementing the investigation, can require the investigated person to undergo specialised medical and psychological examinations and to present the results from them. The investigated person has the right to refuse to undergo the required specialised medical and psychological examinations. The refusal shall be made in writing and the investigation shall be terminated.

(3) The order and the places for implementing the specialised medical and

psychological examinations as well as the regular examinations of the health status according to art. 18, para 1, item 4 and the methods for conducting them shall be determined with an ordinance of the Minister of Health, co-ordinated with SCSI.

Section II. Procedure of investigation

Art. 43.(1) The procedure for investigation for reliability has as objective to establish whether the candidate meets the requirements for issuing of permission for access to classified information.

(2) The procedure for investigation for reliability shall be implemented after written consent of the investigated person.

(3) All the activities for investigation of the person shall be documented.

(4) The written consent of para 2 can be withdrawn at any moment of implementing the procedure for investigation.

(5) At withdrawal of the written consent of para 2 the investigated person does not have right to apply for taking position or for fulfilment of concrete task, connected with work with classified information, for a term of 1 year.

(6) In the cases of para 4 the check shall be terminated immediately. The materials and the documents, conceded by the investigated person shall be returned to him and the data, collected in the progress of the investigation, shall be destroyed by the body, implemented the investigation.

(7) The procedure of para 6 shall be provided with the regulation for implementation of the law.

Art. 44.(1) With objective to be established the reliability for preservation of secret by the investigated person in the progress of the investigation shall be collected data about third persons, pointed out in the questionnaire of the investigated person.

(2) The processing of personal data about the persons of para 1 shall be implemented under the conditions and by the order of the Law for the personal data.

Art. 45.(1) The investigation of art. 43, para 1 shall be implemented for candidates, taking for the first time the positions or implementing the tasks, determined by the order of art. 37.

(2) The investigation of para 1 shall be implemented also for persons, which work requires access to classified information with higher level of classification.

(3) At conducting of competition for taking of position or for fulfilment of concrete task, which require access to classified information, the candidates should meet the requirements of this law for receiving access to the respective level of classified information.

(4) In the announcement for conducting of the competition the requirement of para 3 shall obligatory be pointed out.

(5) The specific requirements about the conducting of the procedure for investigation of the persons of para 3 shall be provided with the regulation for implementation of the law.

Section III. Kinds of investigations

Art. 46. The following kinds of investigations shall be implemented depending on the permitted access:

1. simple investigation – for access to classified information with level of classification "Confidential";

2. expanded investigation – for access to classified information with level of classification "Secret";

3. special investigation – for access to classified information with level of classification "Top secret".

Art. 47.(1) The simple investigation shall be implemented by the employee for the security of the information after written order by the chief of the organisational unit.

(2) In the cases of art. 20, para 3 the investigation shall be implemented by the chief of the organisational unit.

(3) The simple investigation has as objective check of the circumstances art. 40, para 1, items 1 – 5, 7 and 8.

(4) The investigation of para 1 shall include also the filling in of a questionnaire (appendix No 2).

(5) For clarifying the circumstances of para 4 the employee for the security of the information shall have right to require and receive data from the services for public order and from the competent state bodies, and if necessary - to require co-operation from the services for security.

(6) The employee for the security of the information shall finish the investigation and issue or refuse to issue permission for access to information, classified as state secret with level of classification "Confidential" and timely notify SCSI.

Art. 48.(1) The expanded investigation shall be implemented for persons, who apply for positions or for accomplishment of concrete assigned tasks, which impose work with classified information, marked with secrecy grading "Secret".

(2) The investigation of para 1, except the cases of art. 11 and 15, shall be implemented by the National service "Security" upon written request by the chief of the organisational unit, in which the person applies, or which assigns the fulfilment of the task.

(3) The investigation of para 1 has as objective clarification of the circumstances art. 40, para 1.

(4) The investigation of para 1 shall include also the filling in of a questionnaire (appendix No 2).

(5) (amend. SG 31/03) The extended investigation, apart from the circumstances of para 3 and 4, shall include also checks at the place of living, at the place of work, of the bank accounts of the investigated person and in the tax registers, as well as receiving of information from the Agency for financial intelligence.

Art. 49.(1) The special investigation shall be implemented for persons, who apply for positions or for accomplishment of concrete assigned tasks, which impose work with classified information, marked with secrecy grading "Top secret".

(2) The investigation of para 1, except the cases of art. 11 and 15, shall be implemented by the National service "Security" upon written request by the chief of the

organisational unit, in which the person applies, or which assigns the fulfilment of the task.

(3) The special investigation comprises the activities of art. 48, para 3 – 5 and interview both with the investigated person and with three persons, pointed out by him.

Art. 50.(1) In case during the investigation of art. 47, 48 and 49 facts and circumstances are revealed, being obstacle for issuing of permission for the respective level of access, in addition shall be provided interview with the investigated person.

(2) The interview of para 1 has as objective clarification of the revealed facts and circumstances.

(3) Depending on the kind of investigation the interview shall be carried out:

1. for the simple investigation – by the employee for the security of the information, and in the cases of art. 20, para 3 – by the chief of the organisational unt;

2. for the expanded and the special investigation – by the bodies, carrying out the investigation.

(4) The interview of para 1 shall not be carried out, when its conducting may lead to unregulated access to information, classified as state secret.

Art. 51. At the Ministry of Defence and in the Bulgarian Army the investigations of art. 47, para 1, art. 48, para 1 and art. 49, para 1 shall be implemented by the body of art. 11, para 3 after written request by the chief of the respective structural unit.

Section IV. Terms for implementing the investigation or refusal permission to be issued

Art. 52.(1) The investigation for reliability of the person shall be implemented in the following terms:

1. for the simple investigation – up to 30 days after receiving the written order or request;

2. for the expanded investigation – up to 45 days after receiving the written request by the chief of the organisational unit;

3. for the special investigation – up to 60 days after receiving the written request by the chief of the organisational unit.

(2) The respective chiefs can extend the terms of para 1, but with not more than 20 days, on the basis of motivated written application by the employees of the services for security and for public order or by the employees for the security of the information, implementing the investigation, submitted before the elapse of the term.

Art. 53. The State commission for the security of the information, the services of art. 11 and 15 or the employee for the security of the information shall issue or refuse to issue permission for access to classified information of the respective level in 10 days term after the end of the investigation for reliability.

Section V. Issuing, withdrawal, termination and refusal to be issued

permission for access to classified information

Art. 54.(1) Permission for access shall be issued to persons, who meet the requirements of art. 40, para 1, provided for the respective level of classification for security of the information.

(2) The permission for access shall be a written document. The permission shall be issued in three copies according to a model, approved by SCSI, preserved respectively at SCSI, at the service, which has issued it and at the organisational unit.

(3) The permission for access to a higher level of classification shall give right to access also to classified information of lower level, if the access to the lower level of classification is necessary in connection with the taken position or with the accomplishment of concrete assigned task.

Art. 55.(1) The permission for access shall be issued for a term:

1. five years – for level of classification "Confidential";
2. four years – for level of classification "Secret";
3. three years – for level of classification "Top secret".

(2) At least 3 months before the elapse of the terms of para 1 new investigation shall be implemented with regard to the persons, who continue to take the position or to accomplish concrete assigned task, which require access to classified information of certain level.

(3) The investigation of para 2 and the issuing of new permission shall be implemented by the competent bodies under the conditions and by the order of this chapter.

Art. 56.(1) In case about a person, to whom permission has been issued for access to classified information new facts and circumstances become known, which cast doubt about his reliability, the employee for the security of the information shall implement check of these facts and circumstances.

(2) The check of para 1 shall be implemented immediately and has as objective the clarification of the facts and the circumstances of para 1.

(3) The employee for the security of the information shall inform in writing the chief of the organisational unit and the body, issued the permission, about the implemented investigation.

(4) After receiving the written notification the chief of the organisational unit can restrict the access of the investigated person to the respective level of classified information, notifying timely about this the body, issued the permission.

Art. 57.(1) The issuing of permission for access to classified information of certain level shall be refused, when in the progress of the investigation it is established, that:

1. the investigated person does not meet some of the requirements of art. 40, para 1;
2. the investigated person has consciously presented incorrect or incomplete data.

(2) The refusal of issuing of permission shall be prepared in 3 copies according to a model, approved by SCSI, preserved respectively at SCSI, at the body, issued it and at the organisational unit.

(3) The refusal of issuing of permission for access to classified information shall not be motivated, only the legal ground shall be pointed out.

(4) The investigated person shall be informed about the refusal in writing, pointing out the legal ground and a copy of the refusal shall be issued to him.

(5) The refusal to be issued permission for access to classified information shall not be subject to appeal by court order.

(6) An investigated person, to whom has been refused permission for access to classified information, shall not have right to apply for taking a position or for accomplishment of concrete task, connected with work with classified information of the same or of higher level of classification, for a term of one year after the issuing of the refusal.

Art. 58. The permission and the refusal for issuing of permission for access to classified information shall contain:

1. the body, issued the document;

2. name, father name and family name, date and place of birth and UCN of the investigated person;

3. the organisational unit, in which the person applies, works or fulfils contrete task;

4. the kind of the investigation;

5. the level of classification for security of information, to which is permitted or refused access;

6. legal ground for the issuing or the refusal to be issued permission for access to classified information;

7. term of validity of the permission;

8. number of the permission or the refusal;

9. date and place of issuing;

10. signature and seal.

Art. 59.(1) The body, issued the permission for access to classified information, shall withdraw the issued permission upon written proposal by the employee for the security of the information, when:

1. at the check of art. 56 it is established, that the person does not meet some of the requirements of art. 40, para 1;

2. the person has implemented violation of the law or of the by-law acts for its implementation, which has created danger from occurrence or has lead to significant damages for the interests of the state, the organisations or the persons in the field of protection of the classified information;

3. the person has implemented systematic violation of the law or of the by-law acts, connected with the classified information.

(2) The body of para 1 shall immediately notify in writing the chief of the organisational unit or the person about the withdrawal of the permission.

(3) The withdrawal of the issued permission for access to classified information shall not be motivated, only the legal ground being pointed out.

(4) The withdrawal of the issued permission shall be on the basis of a written act with the respective contents of art. 58.

(6) The withdrawal of the issued permission for access to classified information shall not be subject to appeal by court order.

(7) A person, which permission for access to classified information has been withdrawn, shall not have the right to apply for taking position or for accomplishment of

concrete task, connected with work with classified information for a term of three years after the withdrawal.

Art. 60.(1) The body, issued permission for access to classified information, shall terminate the effect of the issued permission upon written proposal by the employee for the security of the information upon:

1. death of the person, received permission for access to classified information;
2. not taking of position or discharge from position;
3. termination of the fulfilment of concrete assigned task;
4. expiry of the terms of art. 55, para 1;
5. change of the need of access to higher level of classification for security of the information.

(2) The body of para 1 shall inform in writing the chief of the organisational unit and the person about the termination of the permission.

(3) The termination of the effect of the issued permission for access to classified information shall not be motivated, pointing out only the legal ground.

(4) The termination of the effect of the issued permission shall be on the basis of written act with the respective content of art. 58.

(5) The termination of the effect of the issued permission for access to classified information shall not be subject to appeal by court order.

Art. 61. In the cases of art. 59 and 60 the employee shall return the issued permission to the body, issued the permission for access to classified information.

Art. 62. The refusal to be issued permission for access to classified information, as well as the termination or the withdrawal of issued permission can be appealed before SCSI in 7 days term after the notification of the person of art. 57, para 4, respectively of art. 59, para 2 and art. 60, para 2.

Art. 63.(1) The appeal shall be submitted in writing through the body, which act is being appealed, to SCSI.

(2) In the appeal shall be pointed out the body, to which it is submitted, the name and the address of appellant, the act, which is appealed against, the body, which has issued it, the complaints and the request of the appellant.

Art. 64.(1) Appeal, submitted after the term of art. 62, shall be returned to the sender against receipt.

(2) In 7 days term after the returning of the appeal can be required restoration of the term, if the missing is due to special unpredicted circumstances. To the request shall be attached the returned appeal.

(3) The request for restoration of the term shall be considered by SCSI. If the request is grounded, the appeal shall proceed and if it is not grounded, the appeal shall be left without considering.

Art. 65.(1) In 7 days term after receiving of the appeal the body, issued the appealed act. can reconsider the problem and issue permission for access to classified information or withdraw the act, with which it has withdrawn the issued permission. In this case the interested shall be notified.

(2) When the body, issued the appealed act does not find ground for re-solving of the issue, it shall send immediately the appeal and the whole file to SCSI.

(7) If in 7 days term after the elapse of the term of para 1 the appeal is not sent to SCSI, appellant can send a copy of the appeal to SCSI or inform it about the admitted delay. SCSI shall require the file officially.

(4) After receiving of the file SCSI can collect new evidence.

Art. 66.(1) The State commission for the security of the information shall decide about the appeal in two weeks term after receiving it.

(2) The State commission for the security of the information shall take decision with which it revokes the administrative act for refusal, termination or withdrawal of issued permission or rejects the appeal.

(3) When the body has unlawfully refused to issue permission for access to classified information, SCSI can oblige this body to start investigation, determining also term for finishing.

Art. 67. In 3 days term after taking the decision the SCSI shall announce it to the appellant, to the body, which act is being appealed and to the organisational unit.

Art. 68. The decision of SCSI shall be ultimate and shall not be subject to appeal.

Art. 69. The refusal, the termination and the withdrawal of issued permission for access to classified information, issued by SCSI, shall not be subject to appeal.

Section VI. Files of the investigations for reliability

Art. 70.(1) The files, containing materials for the investigations for reliability, shall be preserved, maintained, updated, filed and closed by the body, implemented the investigation, separately from the other kinds of files.

(2) The files shall be opened by the competent body at starting the investigation for reliability.

(3) The data, contained in the files, shall be official secret and shall be used for the objectives of this law.

(4) The files of persons, to whom has been issued permission for access to classified information, shall be preserved for a term not longer than five years after the elapse of the term of the permission, after which they shall be destroyed.

Art. 71.(1) The files of the investigated persons shall contain:

1. application for taking position, documents for assigning the accomplishment of

concrete assigned task, requiring access to classified information, respectively application for participation in competition for taking such position or for accomplishment of such task;

2. documents about the individuals or the corporate bodies, applying for concluding or fulfilment of contract, connected with access to classified information;

3. written consent for investigation;

4. written request for investigation;

5. filled in questionnaire;

6. permission, certificate or document for access to classified information;

7. document for refusal, withdrawal or termination of permission for access to classified information;

8. documents for appointment or assigning of concrete task;

9. documents for passed training for protection of compensatory instruments;

10. other documents, containing facts and circumstances, collected under the conditions and by the order of this law.

(2) The special rules for opening, preservation, maintaining, updating, filing and closing of the files for the investigations for reliability shall be determined with the regulation for implementation of the law.

Chapter six. KINDS OF PROTECTION OF THE CLASSIFIED INFORMATION

Section I. Physical security

Art. 72.(1) The physical security of the classified information shall include system of organisational, physical and technical measures for prevention of unregulated access to materials, documents, machinery and facilities, classified as state or official secret.

(2) The system of measures of para 1 shall include the protection of the buildings, the premises and the facilities, where is created, processed and preserved classified information, and the control over the access to them.

Art. 73.(1) The organisational units shall apply system of measures and means for physical security of buildings, premises and facilities, where is created, processed and preserved classified information.

(2) The physical security shall be applied for protection of the classified information from any threat or damage as result of:

1. terrorist activity or sabotage;

2. unregulated access or attempt for unregulated access.

(3) The necessary techniques and means for physical security shall be determined depending on the level of classification and the quality of the classified information, on the number and the level of access of the workers and the employees, determined according to art. 3, on the degree of threat from damaging activities.

Art. 74. For prevention of unregulated access to classified information the chiefs of the organisational units, with the assistance of the employees for the security of the

information, shall:

1. determine the zones for security;

2. determine around the zones for security administrative zones, where is implemented control of people and motor vehicles and which are with the lowest level of security;

3. introduce control regime of entering, movement and exit from for security, as well as obligatory accompanying in these zones of persons without right to access or with right to access to a lower level of classification;

4. ensure respective control over the zones for security and the administrative zones through employees of the units for security and guarding;

5. introduce special regime for preservation of keys from premises, cases and other premises, serving for preservation of classified information.

Art. 75. For ensuring of the protection of the classified information being state security, at meetings, talks, conferences, sessions etc, with subject such information, shall be introduced additional measures for security against listening in on and observation.

Art. 76. The persons, participating in meetings, conferences, sessions, which subject is classified information, which is state secret, shall be checked in advance by the units for security and guarding in the organisational unit.

Art. 77.(1) All materials and technical means, used for protection of classified information, must meet the requirements for stability and undestroyability, corresponding to the level of classification for security of the information, certified by SCSI or by another body, determine with a decision of the Council of Ministers.

(2) Other technical means can be used only as exception, under the condition, that the level, necessary for the given level of classification for security of the information will not be reduced.

(3) The means for physical security, certified for each level of classification, shall be determined in a list, approved by SCSI.

Art. 78. The system of measures, techniques and means for physical security, the conditions and the order for their use, shall be determined with an ordinance of the Council of Ministers.

Art. 79. The employees for the security of the information shall implement preliminary and current control with regard to the organisation, the techniques and the means for physical security in the organisational unit.

Section II. Documentary security

Art. 80.(1) The documentary security shall consist in a system of measures, techniques and means for protection of the classified information at the creating, the

processing and the preservation of documents, as well as at the organising and the work of registries for classified information.

(2) The system of measures, techniques and means for documentary security, the conditions and the order for using them shall be determined with the regulation for implementation of the law.

Art. 81. For ensuring protection of the classified information the chiefs of the organisational units shall determine additional special procedures and requirements within their competence.

Art. 82.(1) Within the organisational unit shall be created separate organisational section – registry for classified information, responsible for the due creating, processing, preservation and submitting to authorised persons of materials, containing classified information. The registries for classified information shall be directly subordinated to the employee for the security of the information.

(2) The requirements for establishing and functioning of the registries of para 1 shall be regulated in the regulation for implementation of the law.

Section III. Personal security

Art. 83.(1) The personal security is a system of principles and measures, applied by the competent bodies by the respective order with regard to persons with objective to be guaranteed their reliability with respect protection of the classified information.

(2) The principles and the measures of para 1 include the principle "need to be known", the procedure for investigation of the persons and the issuing of permission for access under chapter five, the conducting of training of the persons by the order of the law and the regulation for its implementation and the implementing of control in this field.

Section IV. Cryptographic security

Art. 84. Cryptographic security is a system of cryptographic methods and means, which are applied with objective protection of the classified information from unregulated access at its creating, processing, preservation and transfer.

Art. 85. The conditions and the order for the use, the production and the import of cryptographic methods and means for protection of the classified information shall be determined with an ordinance, approved by the Council of Ministers upon a proposal by the Minister of Interior.

Art. 86. For protection of the classified information shall be applied cryptographic methods and means only after preliminary approval and registration by directorate "Protection of the mans for communication" of the Ministry of Interior.

Art. 87.(1) The production and the distribution of the necessary cryptographic keys shall be implemented by directorate "Protection of the mans for communication" of the Ministry of Interior.

(2) The activities of para 1 can be implemented by also other organisational units after the permission and under the control of directorate "Protection of the mans for communication" of the Ministry of Interior.

Art. 88.(1) Within the organisational unit the application of the cryptographic methods and means shall be implemented by the employee for the security of the information or by the other employees of the administrative unit for security, passed training in the field of the cryptographic security and received permission for work with cryptographic means.

(2) The permission of para 1 shall be issued by directorate "Protection of the mans for communication" of the Ministry of Interior after investigation of the persons under art. 46, item 3. The issuing, the termination and the withdrawal of permission shall be implemented under the conditions and by the order of chapter five. The refusal, the termination and the withdrawal shall not be subject to appeal by court order.

(3) The training of para 1 shall be implemented by directorate "Protection of the mans for communication" of the Ministry of Interior or by other organisational units after the permission and under the control of directorate "Protection of the mans for communication" of the Ministry of Interior.

Section V. Security of the automated information systems or networks

Art. 89. The security of the automated information systems (AIS) or networks is a system of principles and measures for protection from unregulated access to the classified information, created, processed, preserved and transferred in AIS or networks.

Art. 90.(1) The obligatory general conditions for security of AIS or networks comprise the computer, the communication, the cryptographic, the physical and the personal security, the security of the information itself on any electronic carrier, as well as the protection from parasitic electromagnetic radiation, determined in an ordinance, approved by the Council of Ministers upon proposal by the Minister of Interior.

(2) The obligatory specific requirements for security of AIS or networks in each organisational unit shall be determined by the chief of the organisational unit upon a proposal by the employee for the security of the information. These requirements shall be subject to approval by directorate "Protection of the means for communications" of the Ministry of Interior.

(3) The requirements of para 2 shall include detail description of the measures for security, which are applied, and the rules for security, which are observed at designing and exploitation of the concrete AIS or network.

(4) The requirements of para 2 shall be prepared at the stage of designing of AIS or networks and if necessary are changed and completed in the process of construction and development of the system.

(5) All following changes in the requirements of para 2 shal be approved by directorate "Protection of the means for communications" of the Ministry of Interior.

Art. 91. Before the introduction in exploitation of AIS or networks directorate "Protection of the means for communications" of the Ministry of Interior shall implement complex assessment of their security according to the requirements of art. 90 and issue a certificate under art. 14, item 2 according to a model, pointed out in the ordinance of art. 90, para 1.

Art. 92. The chief of the organisational unit, in which AIS or networks are used for processing of classified information, upon proposal by the employee for the security of the information, shall appoint or assign to appointed employees of the administrative unit for security and guarding function for the control over the observing of the requirements for security of these systems or networks.

Art. 93. Creating, processing, preservation and transfer of classified information in AIS or networks shall not be admitted without the existing of issued certificate for these AIS or networks by the order of this section.

Art. 94. The connection of AIS or networks, designated for creating, processing, preservation and transfer of classified information with public networks as Internet and similar electronic communication networks shall not be admitted.

Section VI. Industrial security

Art. 95.(1) The industrial security is a system of principles and measures, which are applied with regard to candidates – individuals and corporate bodies, at the concluding of the fulfilment of contract, connected with the access to classified information with objective its protection from unregulated access.

(2) The general requirements for guaranteeing of the industrial security shall be determined on the basis of this law with an ordinance of the Council of Ministers.

(3) Upon proposal of SCSI the Council of Ministers shall determine with a decision the body, conducting the procedure for investigation and issuing certificate for security.

(4) With the contracts of para 1 shall be determined the specific requirements for protection of the classified information, connected with the amount and the level of classification for security, the persons, having access to it, clauses and responsibility in case of not observing of the requirements for industrial security.

Art. 96.(1) Classified information can be conceded only to individuals, to whom have been issued certificates and permissions for access to classified information, and to corporate bodies, to which has been issued certificate for such access.

(2) Out of the cases of para 1, if there is ground to be considered, that in the process of activity a person will create or receive access to classified information, he shall be obliged to require the issuing of permission by the order of chapter five or certificate by the order of this section.

Art. 97.(1) For receiving of certificate an investigation of the candidate shall be implemented at which data shall be collected about:

1. the persons, taking managerial positions, as well as the persons, to whom has been assigned the immediate fulfilment of the contract of art. 95, para 1;

2. the persons, engaged with the conducting of the negotiations, connected with the concluding of the contract of art. 95, para 1;

3. the persons, working in the administrative unit for security of the candidate.

(2) Within the framework of the investigation shall also be collected data about:

1. the structure and the origin of the capital of the candidate;

2. trade partners, financial relations, real rights and other data, necessary for assessment of the reliability of the candidate.

Art. 98.(1) At implementing the investigation the candidate shall fill in questionnaire, determined with the regulation for implementation of the law.

(2) At following occurrence of changes in the data, filled in by the candidate in the questionnaire of para 1, he shall be obliged immediately to inform about this the body, implemented the investigation.

Art. 99. At conceding incorrect data or at not conceding data in the questionnaire of art. 98, para 1 the candidate shall not receive certificate for access to classified information.

Art. 100. Certificate for access to classified information shall be issued to a candidate, who:

1. meets the requirements for security under this law and the acts for its implementation;

2. is economically stable;

3. is reliable from point of view of security.

Art. 101.(1) Not economically stable shall be considered candidate, who:

1. has been announced insolvent or is in procedure for announcing insolvent;

2. has been convicted for bankruptcy;

3. is in liquidation;

4. has been deprived from the right to exercise commercial activity;

5. has liquid and exigible liability to the state, to insurance funds, as well as to individuals and corporate bodies, when it has been recognised before the body for compulsory execution or when it has been established with a court decision, entered into force, with a document, certified by a notary or with security, issued by third person;

6. has been convicted with a sentence entered into force for a crime against ownership or against economy, unless ha has been rehabilitated.

(2) The requirement of para 1, item 6 shall refer also for the managers, respectively the members of the management bodies of the candidates.

(3) The circumstances of para 1 shall be established with a document by the respective competent body.

Art. 102.(1) The candidate shall not be considered reliable from the point of view of security, if:

1. data are established, that he does not meet the requirements of art. 41;

2. it is established, that the persons, pointed out by the candidate for investigation, do not meet the requirements for security of art. 40.

(2) In the cases of para 1, item 2 the candidate can propose other persons.

(3) The investigation of the candidate for reliability from point of view of the security of para 1 shall be implemented by the services for security.

Art. 103.(1) Depending on the results of the conducted investigation the body, who implements it, shall issue certificate for security or refuse to issue it.

(2) Issuing of certificate for security shall be refused, when the candidate does not meet the requirements of art. 100.

(3) The refusal of para 2 shall not be motivated, only the legal ground for issuing being pointed out.

Art. 104.(1) The certificate, as well as the refusal for issuing of certificate for security, shall be issued according to model, approved by SCSI and they shall contain:

1. the competent body;

2. name, headquarters and number of BULSTAT of the candidate, to which shall be issued the certificate or the refusal;

3. the legal ground for issuing of the certificate or the refusal;

4. number of the certificate or the refusal;

5. term of validity of the certificate;

6. date and place of the certificate or the refusal;

7. signature and seal of the body, issuing the certificate or the refusal.

(2) The certificate or the refusal for issuing of certificate shall be written documents and shall be issued in three copies, which shall be preserved at SCSI, at the body, implemented the investigation and at the candidate.

Art. 105. The manager of the organisational unit – assignor under the contract, shall determine a person, who implements control over the observing of the provisions of the law and the acts for its implementation and consult the contractor for the fulfilment of the contract.

Art. 106. The term of the certificate shall be determined depending on the term of the contract, but for not more than three years.

Art. 107. If necessary a new investigation shall be implemented upon application by the candidate, submitted not later than three months before the date of expir of the validity of the certificate in effect to the body, conducted the investigation.

Art. 108.(1) The body, issued the certificate, shall exercise control with objective establishing whether the candidate continues to meet the requirements for security under this law.

(2) In case the persons, received certificate for security, have stopped to meet the requirements of art. 100, item 1, the body, issued the certificate, shall determine a term for removal of the omissions, if they have not lead to unregulated access to classified information.

(3) In case the persons, received certificate for security, have stopped to meet some of the requirements of art. 100, items 2 and 3 and have not removed the omissions within the term of para 2 or it is established, that the offence of art. 100, item 1, has lead to unregulated access to classified information, the certificate for security shall be withdrawn by the body, issued it.

Art. 109. The refusal of art. 103, para 2, as well as the withdrawal of an issued certificate for security shall not be subject to appeal by court order. It shall be appealed by the order art. 62 – 68.

Art. 110.(1) The data, collected at the investigation of a candidate under this section, shall be preserved by the body, implemented the investigation, in a separate file and shall be used with protection as classified information.

(2) The data, contained in the files of para 1, can be used for the objectives of this law.

(3) The file of para 1 shall be preserved for a term of 20 years, assumed from the date of termination of the activity of the candidate.

(4) The special rules for opening, preservation, maintaining, updating, filing and closing of the files for investigation for reliability shall be determined with the regulation for implementation of the law.

Art. 111. The protection of the classified information in the field of the inventions and the useful models shall be implemented in compliance with the provisions of the Law for the patents, unless this law provides other.

Art. 112. The persons of art. 95, para 1 shall, after receiving of certificate for security under this section, have all the obligations of the organisational units under this law.

Chapter seven. CONCEDING OR EXCHANGE OF CLASSIFIED INFORMATION BETWEEN THE REPUBLIC OF BULGARIA AND ANOTHER STATE OR INTERNATIONAL ORGANISATION

Art. 113.(1) The Republic of Bulgaria shall concede or exchange classified information with state or international organisations, with which there are entered into force international agreements for protection of classified information.

(2) If the international agreement of para 1 does not point out which is the applicable law for issues, not provided in it, shall be applied the law of the country – source of the information.

Art. 114. The decision for conceding or exchange of classified information under art.

113, para 1, shall be taken by SCSI on the basis of preliminary statement by the organisational unit, which concedes the information.

Art. 115.(1) In compliance with the concluded international agreement for protection of the classified information SCSI and the competent body for security of the information of the other state or international organisation should on mutual basis establish in advance, that the conceded or exchanged information will be reliably protected.

(2) For the preliminary establishing of the circumstance of para 1 the competent body for the security of the information of the other state or international organisation should ascertain before SCSI, that the persons, who will have access to the conceded or exchanged classified information, are authorised for access to the respective or higher level of classification for security by permission or certificate.

Art. 116. Regarding the exchanged or the conceded to the Republic of Bulgaria classified information on behalf of international organisation, which member is the Republic of Bulgaria, shall be applied the principles, the standards, the procedures for protection of classified information, in effect within this international organisation, if this obligation ensues for the Republic of Bulgaria from its membership in the international organisation.

Chapter eight. ADMINISTRATIVE PUNITIVE PROVISIONS

Art. 117.(1) The one, who violates art. 17, shall be punished with fine from 2000 to 20 000 levs.

(2) When the violation of art. 17 has been made by a corporate body, to it shall be imposed proprietary sanction in amount from 2000 to 20 000 levs.

(3) For admitting the commission of the violation of para 2 the chief of the corporate body shall be punished with fine from 1000 to 5000 levs, if the act does not constitute a crime.

Art. 118.(1) The one, who commits violation of art. 18 and 19 shall be punished with fine from 50 to 300 levs.

(2) The punishment of para 1 shall be imposed to the chief of organisational unit or to an employee for security of the information, who admits commission of violation under art. 18 and 19.

Art. 119. Employee for the security of the information, who commits violation of art. 22, shall be punished with fine from 100 to 1000 levs.

Art. 120.(1) The one, who commits violation of art. 31, shall be punished with fine from 100 to 500 levs.

(2) The punishment of para 1 shall be imposed to the chief of organisational unit or to an employee for security of the information, who admits commission of violation under art. 31.

Art. 121. A person under art. 31, para 1, who commits violation of art. 35, para 4, shall be punished with a fine from 100 to 1000 levs.

Art. 122.(1) An official, who commits violation of art. 43, para 6, shall be punished with fine from 50 to 5000 levs, if the act does not constitute a crime.

(2) The punishment of para 1 shall be imposed to the chief of organisational unit or to an employee for security of the information, who admits commission of violation under art. 43, para 6.

Art. 123. A chief of organisational unit or an employee for security of the information, who commits or admits the commission of violation under art. 73, para 1, shall be punished with fine from 50 to 400 levs.

Art. 124.(1) The one, who commits violation under art. 86, shall be punished with fine from 3000 to 10 000 levs.

(2) When the violation of art. 86 is committed at implementing activity of a corporate body, to it shall be imposed proprietary sanction in amount from 3000 to 15 000 levs.

(3) For admitting the commission of the violation of para 1 the chief of the corporate body shall be punished with fine from 300 to 2000 levs.

Art. 125. A chief of organisational unit, who commits or admits the commission of violation under art. 90, para 2, second sentence, shall be punished with fine from 300 to 2000 levs.

Art. 126. A chief of organisational unit, who commits or admits the commission of violation under art. 92, shall be punished with fine from 500 to 1000 levs.

Art. 127.(1) The one, who commits or admits the commission of violation under art. 93, shall be punished with fine from 500 to 1000 levs.

(2) A chief of organisational unit, who admits the commission of violation under art. 93, shall be punished with fine from 1000 to 2000 levs.

Art. 128.(1) The one, who commits violation under art. 96, shall be punished with fine from 1000 to 3000 levs.

(2) For the violations of para 1 to the corporate bodies shall be imposed proprietary sanction in amount from 1000 to 5000 levs.

(3) Chief of organisational unit and employee for the security of the information, who commits or admits the commission of violation under art. 96, shall be punished with fine from 500 to 1000 levs, if the act does not constitute a crime.

Art. 129.(1) The one, who commits or admits the commission of violation of art. 98, para 2, shall be punished with fine from 500 to 1000 levs.

(2) When the violation of para 1 is committed in implementation of activity of a

corporate body, to it shall be imposed proprietary sanction in amount from 1000 to 5000 levs.

Art. 130.(1) The one, who commits or admits the commission of violation of art. 108, para 3, shall be punished with fine from 500 to 2000 levs, if the act does not constitute a crime.

(2) When the violation of para 1 is committed in implementation of activity of a corporate body, to it shall be imposed proprietary sanction in amount from 1000 to 3000 levs.

Art. 131. A chief of organisational unit, who does not concede information to the competent bodies, required under the conditions and by the order of the law, shall be punished with fine of 500 levs.

Art. 132. In the cases, when for violation of the law and the normative acts for its implementation no other sanction is provided, the guilty shall be punished with fine from 30 to 200 levs.

Art. 133. When the violations of art. 117 – 132 are committed for second time, a fine or proprietary sanction shall be imposed in double extent of the initial one.

Art. 134.(1) The acts for establishing of violations under the previous Art.s shall be compiled by officials, authorised by the chairman of SCSI or the chiefs of the National service "Security" of the Ministry of Interior, service "Security – military police and military counter - intelligence" at the Minister of Defence and directorate "Protection of the means for communication" of the Ministry of Interior, and the punitive decrees shall be issued by the chairman of SCSI or the respective chief of the services, depending on their competence.

(2) The establishing of the violations, the issuing, the appealing and the execution of the punitive decrees shall be implemented by the order of the Law for the administrative violations and penalties.

Additional provisions

§ 1. In the context of this law:

1. "Services for security" are the National intelligence service, the National service for guarding, National service "Security" – MI, directorate "Protection of the means for communication" – MI, directorate "Operational investigation" – MI, directorate "Operational – technical information" – MI, service "Military information" – the Ministry of Defence, and service "Security – military police and military counter - intelligence" – Ministry of Defence.

2. "Services for public order" are the National service "Police" – MI, National service "Fight with organised crime" – MI, National service "Border police" – MI, National service "Gendarmery" – MI, and National service "Fire and accident safety" – MI.

3. "Organisational unit" are: the bodies of the state power and their administrations, including their divisions, parts and structural units, as well as the armed forces of the Republic of Bulgaria, the bodies of the local government and the local administration, the public legal

bodies, established with a law or with act of a body of the executive power, the individuals and the corporate bodies, in which is created, processed, preserved or conceded classified information.

4. "Employee for the security of the information" is an individual, appointed by the chief of the organisational unit for implementing the activity for protection of the classified information in the organisational unit.

5. "Competent body for issuing, terminating, withdrawing and refusing of permission for access to classified information" are SCSI and the chiefs of the services for security and for public order, as well as the employees for the security of the information.

6. "Unregulated access to classified information" is divulging, misuse, change, damage, conceding, destroying of classified information as well as any other actions, leading to damage of its protection or to loss of such information. As unregulated access is considered also any omission to be classified information with marking the respective secrecy grading for security or its incorrect defining, as well as any action or lack of action, lead to knowing by person, who does not have the respective permission or confirmation for this.

7. "Registry" is a special structure, in which is registered, received, sent, distributed, reproduced, conceded and preserved classified information.

8. "Registry in the field of the international relations" is a registry, established by force of international agreement, to which the Republic of Bulgaria is a party.

9. "Secrecy grading" is a marking on a material, containing classified information, showing the level of classification.

10. "Material" is document or any other subject of technical character, facility, equipment, device or armament, produced or in the process of production, as well as component parts of them, used for their production.

11. "Document" is each recorded information, regardless of its physical form or characteristic, including the following information carriers: hand written or typed material, software for data processing, seals, maps, tables, photos, drawings, colours, engravings, plans or parts of them, sketches, working notes, indigo sheet, ink strips or reproduction with whatever means or processes sound, voice, magnetic records, video records, electronic records, optical records in whatever form, portable facilities or devices for automated processing of data with permanent carrier of information or with transportable information carrier etc.

12. "Collection of materials and/or documents" is totality of materials and/or documents, collected together for achieving of objective, provided by the law, referring to one subject and arranged in certain order.

13. "National security" is a status of the society and the state, at which are protected the basic human and civil rights and liberties, the territorial entity, the independence and the sovereignty of the country and is guaranteed the democratic functioning of the state and the civil institutions, as result of which the nation preserves and increases its well-being and is developing.

14. "Interests of the Republic of Bulgaria, connected with the national security" are the guaranteeing of the sovereignty and the territorial entity and the protection of the constitutionally established order in the Republic of Bulgaria, including:

a) revealing, prevention and counteraction to encroachments on the independence and the territorial entity of the country;

b) revealing, prevention and counteraction to secret encroachments, which impede or threaten the political, the economic and the defence interests of the country;

c) receiving of information about foreign countries or of foreign origin, necessary for taking of decisions by the supreme bodies of the state power and the state government;

d) revealing, prevention and counteraction to secret encroachments, directed to forceful change of the constitutionally established order in the country, which guarantees exercising of human and civil rights, democratic representation on the basis of multi – party system and the activity of the institutions, established by the Constitution;

e) revealing, prevention and counteraction to terrorist actions, to illegal traffic of people, arms and drugs, as well as to illegal traffic of products and technologies, placed under international control, money laundering and other specific risks and threats.

15. "Damage in the field of the national security, the defence, the foreign policy or the protection of the constitutionally established order" is threat or damaging of the interests of the Republic of Bulgaria or of these interests, which it has obliged itself to protect, the harmful consequences of which damaging cannot be eliminated, or harmful consequences, which can be alleviated only with following up measures. Depending on the importance of the interests and the gravity of the caused harmful consequences, the damages are irrecoverable or exclusively big, difficult to recover or big and limited, and:

a) irrecoverable or exclusively big damages are these, at which has occurred or could occur full or partial destroying of the national security or the interests of the Republic of Bulgaria, connected with it, as basic protected interests;

b) difficult to recover or big damages are these, at which has occurred or could occur negative impact over the national security or the interests of the Republic of Bulgaria, connected with it, as basic protected interests, which cannot be compensated without occurrence of harmful consequences or the harmful consequences can be alleviated only with significant follow up measures.

c) limited damages are these, at which has occurred or could occur short term negative impact over the national security of the interests of the Republic of Bulgaria, connected with it, as basic protected interests, which may be compensated without occurrence of harmful consequences or the harmful consequences can be alleviated with insignificant follow up measures.

16. "Second" is the violation of the law or the normative acts for its implementation, accomplished in one year term after the punitive decree enters into force, with which is imposed penalty for the same kind of violation.

17. "Systematic violations" are three or more violations of the law or the normative acts for its implementation, accomplished in one year term.

18. "Creating, processing, preservation or conceding of classified information" is the creating, the marking, the registration, the preservation, the registration, the preservation, the use, the conceding, the transformation and the de-classification of classified information.

§ 2. "Official person" in the context of this law is a person of art. 93, item 1 of the Penalty Code.

Temporary and concluding provisions

§ 3. In three months term after the law enters into force the Council of Ministers shall approve Regulation for its implementation.

§ 4. In three months term after the law enters into force the Council of Ministers shall:

1. approve the ordinances of art. 13, art. 78, art. 85, art. 90, para 1 and art. 95, para 2;

2. bring in compliance with this law the Ordinance for the secret patents (SG 81/93) upon a proposal by the chief of the Patent department.

§ 5. In three months term after the law enters into force the Minister of Health, in co-ordination with SCSI issue the ordinance of art. 42, para 3

§ 6. In one month term after the law enters into force the Council of Ministers shall establish State commission for the security of the information and approve structural regulation for its organisation and activity.

§ 7. In three months term after the law enters into force the chiefs of the organisational units shall appoint employees for the security of the information except in the case of art. 20, para 3 and establish the administrative units for the security under the conditions of art. 23.

§ 8. In three months term after the law enters into force the chiefs of the organisational units and the chiefs of the service for security and public order shall compile the lists of art. 37.

§ 9.(1) The materials and documents, prepared till the law enters into force, marked with degrees of secrecy "Top secret of peculiar importance", "Top secret" and "Secret", shall be considered as marked with levels of classification for security respectively "Top secret", "Secret" and "Confidential", the terms being calculated according to art. 34, para 1 and counted from the date of creating them.

(2) In one year term after the law enters into force the chiefs of the organisational units shall be obliged to reconsider and bring in compliance with the requirements of the law and the normative acts for its implementation the materials and the documents, containing classified information.

§ 10.(1) The admissions, issued by the order of the normative acts in effect before the law enters into force, shall preserve their effect till issuing of permissions for access. The chiefs of the organisational units, where work persons with admissions and which positions or concrete assigned tasks require work with classified information, shall be obliged to require issuing of permission for access in compliance with the requirements of the law in 3 months term after it enters into force. The non fulfilment of this obligation shall lead to termination of the effect of the already issued admissions.

(2) The procedure for investigation and issuing of the permissions of para 1 shall finish within term, determined by SCSI, but not later than 18 months.

§ 11. (corr. SG 5/03) The procedures for issuing of admission for work with secret information, found in procedure of investigation, shall be transformed in procedure for

investigation, implemented under the conditions and by the order of the law.

§ 12. In the Law for the cadastre and the property register (SG 34/00) in art. 20, para 1, item 2 the words "to preserve as official secret the data, which have become known to him" shall be substituted by "to protect the classified information, being official secret, which have become known to him".

§ 13. In the law for the Constitutional Court (prom. SG 67/91; amend. SG 25/01) in art 20 the following amendments and supplements:

1. In para 2 the words "state, or official secret" shall be substituted by "classified information, being state or official secret".

2. Para 3 shall be created:

"(2) In the case of para 2 shall be observed the conditions and the order of the Law for the protection of the classified information".

§ 14. In the Law for the armed forces of the Republic of Bulgaria (prom. SG 112/95; amend. and suppl. SG 67/96, SG 122/97, SG 70, 93, 152, 152, 153/98, SG 12, 67, 69/99, SG 49, 64/00, SG 25/01, SG 1, 40/02) the following amendments shall be made:

1. In art. 5 the words "the state and the official secret" shall be substituted by "classified information, being state and official secret".

2. In art. 32 item 9 shall be repealed.

3. In art. 35, para 1, item 14 the words "the state and official secret" shall be substituted by "classified information, being state and official secret".

4. In art. 78, para 1, item 16 the words "the state and official secret" shall be substituted by "classified information, being state and official secret".

5. In art. 200 the words "state or official secret" shall be substituted by "classified information".

6. In art. 273 the words "state or official secret" shall be substituted by "classified information".

7. In art. 281, item 1 the words "the state and official secret" shall be substituted by "classified information, being state and official secret".

§ 15. In art. 9, para 2 of the Currency law (SG 83/99) the words "and official secret" shall be substitute by "secret and the requirements for protection of the classified information, being official secret".

§ 16. In at. 3, para 3 of the Law for the automobile transport (prom. SG 82/99; amend. SG 11/02) the word "official" shall be substituted by "classified information being official secret".

§ 17. In art. 15, para 3 of the Law for the administrative procedures (Prom. SG 90 1979; Amend. SG 9 1983; Amend. SG 26 1988; Amend. SG 94 1990; Amend. SG 25 1991; Amend. SG 61 1991; Amend. SG 19 1992; Amend. SG 65 1995; Amend. SG 70 1995; Amend and Suppl SG 122 1997; Amend. SG 15 1998; Amend. SG 83 1999; Amend. SG 95 1999) the

words "with protection of" shall be substituted by "with protection of classified information, being".

§ 18. In § 5 of the additional procedures of the Law for the refuges (prom. SG 53/99; corr. SG 97/99) the words "official secret" shall be substituted by "classified information, being official secret".

§ 19. In art. 52 of the Law for the banks (Prom. SG 52 1997; Suppl. SG 15 1998; Amend. SG 21 1998; Suppl. SG 52 1998; Amend. SG 70 1998; Amend. and Suppl. SG 54 1999; Amend. SG 103 1999; Amend. SG 114 1999; Amend. SG 1 2000; Amend. SG 24 2000;Amend. SG 63 2000; Amend. and Suppl. SG 84 2000 ; Amend. SG 92 2000; Amend., SG 1 2001) para 8 shall be created:

"(8) Upon written request of the chairman of the SCSI or of the chiefs of the security services and of the public peace services the banks shall be obliged to submit information for the bank accounts and the operations on the accounts and the savings of persons subject to investigation for reliability, under the conditions and by the order of the Law for protection of the classified information. The request shall be accompanied by a consent of the investigated person for the disclosure of this information".

§ 20. In the Law for the Bulgarian identification documents (Prom. SG 93 1998; Amend and Suppl SG 53 1999; Amend. SG 67 1999; Amend. SG 70 1999; Amend. SG 113 1999; Amend. and Suppl. SG 108 2000; Amend. and suppl., SG 42 2001) the following amendments and supplements shall be made:

1. in art. 75 new item 2 shall be created:

"2. persons, for whom enough evidence exists that by their travelling they threaten the system of protection of the classified information representing a state secret of the Republic of Bulgaria;".

2. In art. 78 the previous text shall become para 1 and para 2 shall be created:

"(2) The compulsory administrative measure under art. 75, item 2 shall be applied by a motivated order of the chairman of the State Commission for the security of the information or of the chiefs of the security services and the public order services."

In art. 79, para 1 and 2 the words "art. 75, items 1 and 3" shall be substituted by "art. 75, items 1 - 3".

§ 21. In the Law for the Ministry of Interior (Prom. SG 122 1997; Amend. SG 29 1998; Amend. SG 70 1998; Amend. and Suppl. SG 73 1998; Amend. and Suppl. SG 153 1998; Amend. SG 30 1999; Amend. SG 110 1999; Amend. SG 1 2000; Amend. SG 29 2000; Amend. and Suppl. SG 28 2001) the following amendments shall be made:

1. In art. 7, item 14 the words "ciphering work in the Republic of Bulgaria and its foreign representations" shall be substituted by "the cryptographic protection of the classified information in the Republic of Bulgaria and in its diplomatic and consular representations".

2. In art 46, para 1, item 7 the words "protection of the facts, the information and the subjects, being state secret" shall be substituted by "protection of the classified information, being state or official secret".

3. In art. 51, para 1 shall be changed to:

"(1) The national office "Security" shall carry out activity in connection with the functioning of the national system for protection of the classified information representing state or official secret according to the Law for protection of the classified information."

4. In art. 52, para 1 the words "protection of the facts, the information and the subjects, being state secret" shall be substituted by "protection of the classified information".

5. Art. 53 shall be revoked.

6. Art. 124 shall be changed to:

"Art. 124. Directorate "Protection of the communication devices" is a specialised unit of MI for cryptographic protection of the classified information in the Republic of Bulgaria and in its diplomatic and consular representations, for acquiring, systematising and processing of information from foreign sources to the interest of the state security and operative control over the radio frequency spectrum by:

1. assessing and working out cryptographic algorithms and devices for cryptographic protection of the classified information; working out and distributing the used cryptographic keys; permitting and controlling the using, the production and the import of devices for cryptographic protection;

2. issuance of certificate for security of the automated informational systems or networks used for work with classified information; co-ordination and control of the activity on the protection of the technical devices against parasitic electromagnetic emissions of the technical devices processing, storing and transferring classified information;

3. organise and provide the communications of the Republic of Bulgaria with its diplomatic and consular representations and the cryptographic protection of the exchanged information providing the necessary personnel in the administrative units and in the diplomatic and consular representations;

4. acquire, process and systematise information by technical devices from technical sources of other countries to the interest of the national security and submit it to users determined by an order of the Minister of the Interior and by a law;

5. detect and prevent the use of the national radio frequency spectrum against the security of the country or in violation of the laws and interact with the competent state bodies;

6. provide and apply special reconnaissance devices and prepare material evidence under conditions and by an order determined by a law;

7. carry out operative and investigation activity;

8. interact with the other offices of MI and with the specialised state bodies, as well as with related offices of other countries, within the circle of their competence;

9. carry out informational activity.

(2) The administrative bodies shall provide financially the activity of the units under para 1, item 3 and in the diplomatic and consular representations.

(3) The organisation of the activity under para 1, item 3 shall be determined by an ordinance of the Council of Ministers."

7. In art. 162 para 3 shall be revoked.

8. In art. 187, the words "protection of the data and the information, being state secret" shall be substituted by "protection of the classified information".

§ 22. In the Law for the Bulgarian National Bank (prom. SG 46/97; amend. SG 49, 153/98, SG 20, 54/99, SG 109/01) the following amendments and supplements shall be made:

1. In art. 4, para 2 after the words "the credit relations" a comma shall be put and shall

be added "except the cases, provided in the Law for the classified information"

2. In art. 23, para 2 the words "which are official and" shall be substituted by "which is classified information, being official secret or".

§ 23. In the Law for access to public information (prom. SG 55/00;amend, SG 1/02) the following changes shall be made:

1. In art. 7, para 1 the word "constitute" shall be substituted by "classified information, constituting".

2. In art. 9, para 2 the words "state or official secret" shall be substituted by "classified information, constituting state of official secret".

3. In art. 13, para 3 the words "20 years" shall be substituted by "2 years".

4. In art. 37, para 1, item 1 the words "state of official secret" shall be substituted by "classified information, constituting state of official secret".

5. In art. 41, para 4 the word "classifying" shall be substituted by "marking with secrecy grading".

§ 24. In the Law for the state ownership (prom. SG 44/96; amend. SG 104/96, SG 55, 61, 117/97, SG 93, 124/98, SG 67/99, SG 9, 12, 26, 57/00, SG 1/01, SG 38/01 – Decision of the Constitutional Court of 2001) the following amendments shall be made:

1. In art. 70, para 2 the words "state secret" shall be substituted by "classified information, being state secret".

2. In art. 78, para 2 the words "state secret" shall be substituted by "classified information, being state secret".

§ 25. In the law for the civil servant (prom. SG 67/99; amend. SG 1/00, SG 25, 99, 110/01) art 25 shall be changed to:

"Art. 25. The civil servant shall be obliged to protect the classified information representing state or official secret that have become known to him at or on the occasion of fulfilment of his official duties.

(2) The classified information representing state or official secret, as well as the order of working with it shall be determined by a law."

§ 26. In the Law for restoration of the ownership of forests and the lands of the forest entirety (prom. SG 110/97; amend. SG 33, 59, 133/98, SG 49/99, SG 26, 36/01) in art. 17 the following amendments and supplements shall be made:

1. The previous text shall become para 1 and in it the words "including also these, constituting state secret" shall be deleted.

2. Para 2 shall be created:

"(2) In the cases, when the information of para 1 is classified information, it shall be conceded under the conditions and by the order of the Law for the protection of the classified information."

§ 27. In the Law for the postal services (prom. SG 64/00; amend. SG 112/01) in art. 11, para 1 the words "secret correspondence" shall be substituted by "correspondence,

containing classified information".

§ 28. In Edict No 612 for the seals (prom. SG 69/65; amend, SG 26/88, SG 11, 47/98) in chapter two at. 49 shall be revoked.

§ 29. In the Law for public procurement (Prom. SG 56 1999; Amend. SG 92 2000; Suppl. SG 97 2000; Amend. and suppl. SG 43 2002) in art. 6, item 1 the words "are subject to state secret" shall be substituted by "are subject of classified information, constituting state secret."

§ 30. In the law for the statistics (Prom. SG 57 1999; Amend. and Suppl. SG 42 2001) the following amendments shall be made:

1. In art. 22 the words "protection of the secret" shall be substituted by "protection of the classified information".

2. In art. 27 para 2 shall be changed to:

"(2) The registration, the using, the processing and the storing of data representing classified information shall be carried out in compliance with the requirements of the normative acts for protection of the classified information."

§ 31. In the law for the audit office (SG 109/01) the following amendments and supplements shall be made:

1. In art. 30, para 1 the words "the state, the official" shall be substituted by "the classified information, constituting state or official secret, as well as".

2. In art. 31 para 7 shall be created:

"(7) When, in exercising the capacity under para 1, access is necessary to classified information observed shall be the conditions and the order of the Law for protection of the classified information."

§ 32. In the law for transformation of the Construction Forces, the forces of the Ministry of transport and the Forces of the Committee for posts and telecommunications into state enterprises (SG 57/00)in art. 6, para 2 the second sentence shall be changed to:

"They can fulfil and assign public procurement connected with the defence of the country and the security of the country which are subject to classified information representing state secret whose accomplishment shall be carried out under conditions and by order of the Law for protection of the classified information."

§ 33. In the law for social support (SG 56/98) in art. 32 para 2 shall be changed to:

"(2) The inspectors shall be obliged to observe the normative requirements for protection of the classified information that has become known to them at and in connection with the implemented checks as well as to respect the honour and the dignity of the supported persons."

§ 34. In the Law for the patents (Prom. SG 27 1993; Suppl. SG 83 1996; Amend. SG

11 1998; Amend. and Suppl. SG 81 1999) the following amendments shal be made:

1. Art. 24 shall e changed to:

"Art. 24. (Amend., SG 45/02) (1) Classified patents shall be issued for inventions containing classified information representing state secret in the context of art. 25 of the Law for protection of the classified information.

(2) In filing application for secret patent the applicant shall be obliged to declare that the invention does not represent a state secret.

(3) The level of classification for security reasons of an invention by an application according to para 2 shall be determined by the respective competent body to whose activity the invention is related upon coordination with the State Commission for the security of information.

(4) The competent body under para 3 shall announce its decision within 3 months from its approaching and shall inform about that the Patent Office. Placed on the application for classified patent with a definite level of classification for security shall be a respective grading, informing about that the applicant.

(5) If, within the period under para 4, the Patent Office does not receive information about the level of classification for security of the invention it shall be considered that the application does not contain classified information representing state secret. The Patent Office shall inform the applicant that the invention of the application for classified patent does not contain classified information representing state secret, and shall require his explicit consent to consider the application by the general order. If he does not express consent the application shall be considered withdrawn and the materials shall be returned.

(6) If the competent body under para 3 is an applicant and, upon coordination with the State Commission for the security of information, the application is marked by security grading according to a level of classification for security of the invention the procedure under para 4 and 5 shall not apply.

(7) The Patent Office shall publish only the numbers of the issued classified patents for which fee shall not be due."

2. In art. 25 para 2 shall be changed to:

"(2) The competent bodies under art. 24, para 3, upon co-ordination with the State Commission for the security of information, can prohibit patenting abroad of inventions containing classified information representing state secret."

3. In art. 31, para 5 the words "after preliminary written consent of the Ministry of Defence of the Ministry of Interior" shall be substituted by "under the conditions and by the order of the Law for protection of the classified information".

4. In art. 32, para 8 the words "only by the Council of Ministers upon request by the Ministry of Defence of the Ministry of Interior" shall be substituted by "by the State commission for the security of the information".

5. In art. 45, para 3 the words "the Ministry of Defence of the Ministry of Interior" shall be substituted by "with the competent bodies of art. 24, para 3 after co-ordination with the State commission for the security of the information".

6. In art. 46 para 3 shall be repealed.

7. In art. 48 the words "art. 46, para 1, 2 and 3" shall be substituted by "art. 46, para 1 and 2".

8. In art. 50 the following amendments shall be made:

a) in para 1 item 3 shall be changed to:

"3. the application is for a classified patent for invention containing classified

information representing state secret;";

b) para 3 shall be changed to:

"(3) The Patent Office shall make a publication when, by the order of art. 34 of the Law for protection of the classified information, have dropped the legal grounds for classifying the information contained in the invention as a state secret."

9. In art. 55, para 1, item 1 the words "art. 46, para 2 and 3" shall be substituted by "art. 46, para 2".

10. In art. 67 para 6 shall be changed to:

"(6) In the cases of self indication of the Republic of Bulgaria according to art. 8, para 2, letter "b" of the Treaty the Patent Office shall send the international application to the competent bodies to whose activity the invention is related for determining the level of classification for security. The determination of the level of the classification for security of the invention of the application shall be carried out under the conditions and by the order of the Law for protection of the classified information and by the deadline under art. 24, para 4 of this law. Should it be established that the international application contains information classified as a state secret it shall not be treated as international, shall not be sent ex-officio and shall not be published."

11. In art. 84, para 1 the words "secret order" shall be substituted by "order for patent" and the words "from 100 to 1000 levs" shall be substituted by "from 1000 to 20 000 levs".

§ 35. In the Law for the telecommunications (Prom. SG 93 1998; Amend. and Suppl. SG 26 1999; Amend. and Suppl. SG 10 2000; Amend. and Suppl. SG 64 2000; Suppl. SG 34 2001; Amend. and Suppl. SG 42 2001; Amend. and Suppl. SG 96 2001; Amend. and Suppl. SG 112 2001) in art. 99, para 1 the words "national cipher body" shall be substituted by "directorate "Protection of the means for communication".

§ 36. In the Law for the local government and the local administration (Prom. SG 77 1991; Amend. SG 24 1995; Amend. SG 49 1995; Amend. SG 65 1995; Amend. SG 90 1996; Suppl. SG 122 1997; Amend. SG 33 1998; Amend. SG 130 1998; Amend. and Suppl. SG 154 1998; Suppl. SG 67 1999; Amend. and Suppl. SG 69 1999; Amend. SG 26 2000; Amend. and Suppl. SG 85 2000; Amend. SG 1 2001; Suppl., SG 28 2002) in art. 33, para 2 the words "state or official secret under a law" shall be substituted by "classified information, constituting state or official secret".

§ 37.(1) This law shall revoke the Law for access to the documents of the former State security and the former Intelligence department of the general staff (prom. SG 63/97, SG 89/97 – Decision No 10 of the Constitutional Court of 1997; amend. SG 69/99, SG 24/01, SG 51/01 – Decision No 14 of the Constitutional Court of 2001; amend. SG 28/02).

(2) The resources, provided under the Law for the state budget for 2002, as well as the long term material assets of the state bodies, terminated their activity under the Law for access to the documents of the former State security and the former Intelligence department of the general staff shall be conceded to the State commission for the security of the information.

§ 38. In the Penalty Code (Prom. SG 26 1968; Corr. SG 29 1968; Amend. and Suppl. SG 92 1969; Amend. and Suppl. SG 26 1973; Amend. and Suppl. SG 27 1973; Amend. and

Suppl. SG 89 1974; Amend. and Suppl. SG 95 1975; Amend. and Suppl. SG 3 1977; Amend. and Suppl. SG 54 1978; Amend. and Suppl. SG 89 1979; Amend. and Suppl. SG 28 1982; Corr. SG 31 1982; Amend. and Suppl. SG 44 1984; Amend. and Suppl. SG 41 1985; Amend. and Suppl. SG 79 1985; Corr. SG 80 1985; Amend. and Suppl. SG 89 1986; Corr. SG 90 1986; Amend. SG 37 1989; Amend. SG 91 1989; Amend. SG 99 1989; Amend. SG 10 1990; Amend. SG 31 1990; Amend. SG 81 1990; Amend. SG 1 1991; Amend. SG 86 1991; Corr. SG 90 1991; Amend. SG 105 1991; Suppl. SG 54 1992; Amend. SG 10 1993; Amend. SG 50 1995; Amend. SG 97 1995; Amend. SG 102 1995; Amend. SG 107 1996; Amend. and Suppl. SG 62 1997; Amend. and Suppl. SG 85 1997; Amend. SG 120 1997; Suppl. SG 83 1998; Amend. and Suppl. SG 85 1998; Suppl. SG 132 1998; Amend. SG 133 1998; Amend. and Suppl. SG 153 1998; Amend. and Suppl. SG 7 1999; Amend. SG 51 1999; Amend. and Suppl. SG 81 1999; Amend. and Suppl. SG 21 2000; Amend. and Suppl. SG 51 2000; Amend. SG 98 2000; Suppl. SG 41 2001; Amend. SG 101 2001) art. 284a and 313 b shall be revoked.

§ 39. In the law for election of people's representatives (Prom. SG 37 2001; Amend., SG 44 2001) art. 24, para 1, items 9 and 10, art. 29, para 2, art. 48, para 5 and § 6 of the transitional and concluding provisions shall be revoked.

§ 40. In the Law for election of Great National Assembly (prom. SG28/90; amend. SG 24/01) art. 42a shall be revoked.

§ 41. In the Law for election of President and vice President of the republic (Prom. SG 82 1991 ; Amend. and Suppl. SG 98 1991 ; Amend. and Suppl. SG 44 1996 ; Amend. SG 59 1998 ; Amend. and Suppl. SG 24 2001 ; Amend. and Suppl. SG 80 2001; Amend. SG 90 2001) in art. 8 para 2 shall be revoked.

§ 42. In the law for the local elections (prom. SG 66/95; corr. SG 68/95, SG 85/95 – Decision No 15 of the Constitutional Court of 1995; amend. SG 33/96, SG 22/97 - Decision No 4 of the Constitutional Court of 1997; amend. SG 11, 59/98, SG 69, 85/99, SG 29/00, SG 24/01) in art. 42 para 4 shall be revoked.

§ 43. This law shall revoke the List of the facts, data and subjects, constituting state secret of the Republic of Bulgaria (prom. SG 31/90; amend. SG 90, 99/92, SG 108/99, SG 55/00).

The law was passed by the 39th National Assembly on April 24, 2002 and is affixed with the official seal of the National Assembly.

List of the categories of information, subject to classification as state secret

I. Information, connected with the defence of the country

1. Structure, organisation and functioning of the state bodies and of the Supreme command of the Armed Forces of the Republic of Bulgaria in state of war, martial law or other emergency status.

2. Location, equipment, maintenance, exploitation and organisation of the guard of the command points of the central and the territorial administration of the executive power and

of the Armed forces of the Republic of Bulgaria, designated for use in state of war, martial law or other emergency status.

3. Organisation and functioning of the communication and information systems for communication of the bodies of state government and of the Armed forces of the Republic of Bulgaria at different status and degrees of combat readiness and war.

4. Data about bringing the state in higher state and degrees of combat readiness, the war time plans and estimates, projects and measures, connected with the ensuring of the defence ability at national level of the central and the territorial administration of the executive power and of the commercial companies, producing military production. Information about the planning, the organisation and the functioning of the mobilisation deployment of the Armed Forces of the Republic of Bulgaria.

5. Detailed structure of the armed forces, as well as data about the places of location (dislocation) and their movement (re-dislocation), the actual name, the organisation, the payroll and the list numbers of the personnel, the armament and the systems for management of the Armed Forces of the Republic of Bulgaria, of the separate kinds of armed forces, types and special forces, unions, formations, regime divisions and sites, not included in the official exchange of data, ensuing from international obligations of the state.

6. Information about the tasks and the combat abilities of the Armed forces of the Republic of Bulgaria, of the separate kinds of armed forces, types and special forces as well as of the potential adversary and the envisaged regions and directions of the military actions.

7. Organisation, functions and technical means for electronic reconnaissance.

8. Organisation and functioning of the system of bringing of the armed forces, of the central and the territorial administration of the executive power and of the obliged corporate bodies in higher state and degrees of combat readiness.

9. Strategic and operational documents in which are established the concepts accepted by the armed forces for leading the war and the operations.

10. Information, referring to foreign treats and dangers of military characteristics, defence plans, analyses and prognoses, as well as the decisions and tasks ensuing from them.

11. Data about the designing, the trial, the accepting as armament of new models of armament, combat machinery and ammunitions and the created mobilisation capacities for their production.

12. Data about the planning and the ensuring of the common war time plan with material, financial and labour resources, as well as the decisions and the tasks, ensuing from them.

13. Organisation, dislocation, armament, tasks and capacity of the bodies for reconnaissance.

14. Data about the communication system and distribution of the frequencies of the radio communications of the Republic of Bulgaria, which are connected with the defence and the security.

15. Plans and accounts of the leaves and the spent material resources, connected with concrete missions and tasks for the defence of the country, defined with an act of the Council of Ministers.

16. Plans, data and summarised data about the status of the operational readiness of the territory of the country and the construction of new sites with war time designation.

17. Summarised information about the special production of the defence industry, as well as prognoses for the development, the plans, the production capacity, the scientific and the research units for realisation of orders for armament, combat machinery, ammunitions and

military equipment.

18. (supppl., SG 52/04) Geodetic and cartographic materials and data, digital models and data, raster images, air photographs and photo documents, containing information about the location, the kind, the character, the designation or the engineering equipment of the sites and the regions, having importance for the defence and the security of the country, with exception of those related to the safety of the air navigation in the coordinate system WGS-84.

19. Tasks of the central and the territorial administration of the executive power and of the obliged corporate bodies in state of war, martial law or other emergency status.

20. Organisation, functioning and management of the system for supply of the Armed forces of the Republic of Bulgaria with material means in state of war, martial law or other emergency status.

21. Data about the strategic stores of material means, created for war time.

22. Summarised data about the import and the export of arms, combat machinery and ammunitions for the needs of the Armed Forces of the Republic of Bulgaria.

23. Planning, realisation and results of the scientific and research activity with particular importance for the defence and the security of the Republic of Bulgaria.

24. Summarised data about the relief and the character (the structure)of the sea and the river bottom. The elements, which determine the hydrologic regime of the coastal waters in real time (except the water ways, announced for international sailing). Data about the established places for crossing of the rivers by the troops in the Republic of Bulgaria.

II. Information, connected with the foreign policy and the internal security of the country

1. Information from the field of the foreign policy, unregulated access to which would seriously threaten the national security or could damage or create danger of occurrence of significant damages of the positions of the country in negotiations with another state.

2. Data and documents about the internal political and the military status of other states, based on not published data, which divulging can threaten the national security of the country.

3. Data about the organisation, the techniques and the means at fulfilment of specific tasks, implemented through the operational - investigating and the operational - intelligence activity of the services for security and public order, as well as data about their special facilities and the information, received as result of this activities and subjects, as well as data, allowing to be established persons, rendered or rendering support in these activities.

4. Detailed organisation and payroll structure of the services for security and public order, as well as summarised data about the personnel.

5. Establishing data or data, which can help for the establishing of persons, who are not employees, but co-operate or have co-operated with the services for security and services for public order.

6. Information about special reconnaissance means, used according to the law (technical means and/or the techniques for their application).

7. Data about the kind, the level of supply and the qualities of special machinery, armament, ammunitions, defence resources, devices and materials, used by the services for security and by the services for public order.

8. Data, received as result of using of special reconnaissance means and data about the controlling of purchases and secretly overviewed shipments.

9. Reports, accounts, information bulletins, statistical and other data about the operational work of the services for security and the services for public order.

10. Information about released and used budget resources and state property for special means, connected with the national security.

11. The unified registers of the permissions, the certificates or the refusals of access to classified information and the files for investigation about reliability, kept and preserved by SCSI.

12. The information, connected with the working out and the preservation of the seals with images of the state emblem as well as of the seals of the bodies of the state power.

13. Classified information, exchanged between the Republic of Bulgaria and international organisations or states, marked with secrecy grading for security "Top secret", "Secret", "Confidential" or equal to it.

14. Data about the organisational - technical and the software protection of the automated information systems or networks of the bodies of state power and the local government and their administrations.

15. Information about designing, supply with equipment of telecommunication, tele-information and post networks for transfer of classified information, being state secret, used for the needs of the armed forces, the services for security or the organisations for ensuring these systems and networks.

16. Passwords, and codes for access to devices, creating, processing, preserving and transferring information, marked with secrecy grading "Top secret", "Secret" or "Confidential".

17. Organisations, methods and means for cryptographic protection of classified information, marked with secrecy grading "Top secret", "Secret" or "Confidential"; description and samples of means, developed or used for cryptographic protection of the such classified information; key materials and classified information, protected with cryptographic methods and means.

18. Information about the passing of the economy from peace to war time status under the different states and degrees of combat readiness and in the state of war.

19. Information about the preparation, the organisation and the use of the railway, the road and the water transport at bringing of the state and the Armed Forces of the Republic of Bulgaria into a higher status and degrees of combat readiness.

20. information about the organisation, the methods and the resources, servicing for the preservation of the classified information, constituting state secret.

21. information about the location, the designation, the planning and the supply of sites with special designation, as well as plans for their defence and guarding.

22 Information about persons, suspected for conducting of subversive, terrorist or other illegal activity against the security, the defence, the independence, the entity or the international status of the state, received, checked and analysed by the services for security and the services for public order.

23. The system of forms and methods for preservation, as well as the operational opportunities for the guarding of the state border, the activity of the border control check-points as well as information about anti-terrorist anti-sabotage activities at the state border.

24. Summarised data, referring to the functioning of the system for protection of the classified information, constituting state secret.

25. Electronic registers and diaries for registration of documents, as well as lists of other materials, containing classified information, constituting state secret.

26. Materials of the Council of Ministers, concerning the strategic potential of the state, as well as government strategic orders, connected with the national security and their realisation.

27. Information about the production technology, as well as separate ways of protection of identity documents, bank-notes and other securities and means for payment as well as other protected (from falsifying) documents, issued by the bodies of the state power and their administrations.

28. Information about plans and tasks of the foreign policy, which divulging would damage important interests of the state till the time of their official announcement.

29. Materials, documents, report notes from international negotiations and consultations, as well as international agreements or parts of them, if they are classified information.

30. Organisation and functioning of the diplomatic post.

31. System of guarding of the Bulgarian diplomatic and consular representations.

32. The tasks of the Bulgarian diplomatic and consular representations in time of war.

33. The tasks for guarding of foreign diplomatic and consular representations as well as representations of international organisations in the Republic of Bulgaria in the time of war.

III. Information, connected with the economic security of the country

1. Documents, about negotiations for concluding of financial agreements of state importance, which divulging would damage the national security.

2. The research work with particular essential importance for the interests of the national economy, ordered by state bodies.

3. Information about technical, technological and organisational decisions, which divulging could threaten with damaging of important economic interests of the state.

4. Information about the way of action of control - signalling devices, alarm systems and the regime of guarding, which knowing could damage the national security.

5. Political, economic or military information, referring to foreign countries, received under the condition, that classified information will be protected.

6. Plans, prognoses and information about the development of the turnover with special equipment, special technologies and special services wit other states.

7. Information about inventions or useful models, determined as concerning the security and the defence of the country, according to the Law for the patents.