Protection of Classified Information Act

Promulgated, SG No. 45/30.04.2002, Corrected, SG No. 5/2003, Amended, SG No. 31/4.04.2003, supplemented, SG No. 52/18.06.2004, No. 55/25.06.2004, SG No. 89/12.10.2004

Chapter One

GENERAL PROVISIONS

Article 1

(1) This Act governs the public relations arising in connection with the generation, the processing, and the storing of classified information, and lays down the conditions and procedure for the release thereof and the access thereto.

(2) The purpose of this Act is to protect classified information from unauthorised access.

(3) Within the meaning of this Act, "classified information" is any information which is a State secret or an official secret, and any foreign classified information.

Article 2

This Act shall apply as well to any foreign classified information which may be made available by another State or an international organisation, insofar as an existing international treaty, to which the Republic of Bulgaria is a party, does not provide otherwise.

Article 3

(1) Access to classified information shall not be allowed to any person other than those having an appropriate clearance in keeping with the "need- to-know" principle, unless otherwise provided hereunder.

(2) The "need-to-know" principle is the restriction of access to particularclassified information to such persons whose official duties, or a special assignment, require such access.

Chapter Two

CLASSIFIED INFORMATION PROTECTION AUTHORITIES

Section I

State Information Security Commission

Article 4

(1) The State Information Security Commission (SISC) is a government authority which shall conduct the classified information protection policy of the Republic of Bulgaria.

(2) The State Information Security Commission is a first-tier obligor of budget funds.

Article 5

The State Information Security Commission shall be supported by an administration of which the activities, structure and operation shall be laid down in Institutional Rules adopted by the Council of Ministers.

Article 6

(1) The State Information Security Commission is a collegiate body comprised of five members, including a chairperson and a vice chairperson, who shall be appointed by the Council of Ministers for a term of five years, subject to the advice of the Prime Minister.

(2) No person may be a member of the Commission unless such person is a university graduate.

Article 7

(1) The SISC chairperson shall submit an annual report to the Council of Ministers on the overall activity relating to the protection of classified information.

(2) The Council of Ministers shall introduce the report under paragraph 1 before the National Assembly, which shall adopt it by its decision.

(3) The SISC chairperson shall provide the same volume and content of information on the Commission's activities to the Speaker of the National Assembly, to the President of the Republic, and to the Prime Minister.

Article 8

The State Information Security Commission shall have a duty to:

1. organise, perform, coordinate and control the activities relating to theprotection of classified information;

2. provide equal protection of classified information;

3. perform its activities in close collaboration with the authorities of the Ministry of Defence, of the Ministry of Home Affairs, of the Ministry of Foreign Affairs, and with the security services and the public order services.

Article 9

For the purposes of performing its activities, SISC shall have a duty to:

1. develop guidelines and approve plans of action for organisational units in the event of a threat to the interests of the State resulting from unauthorised access to classified information;

2. analyse and assess the state of preparedness for the protection of classified information in the event of a threat to any interest protected by law resulting from unauthorised access to classified information, and shall issue mandatory instructions in that area;

3. organise and perform activities to prevent and mitigate the harmful consequences of unauthorised access to classified information;

4. draft and introduce before the Council of Ministers for adoption statutory instruments relating to the protection of classified information;

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

6. organise, control, and be responsible for, the performance of obligations relating to the protection of classified information as laid down in international treaties to which the Republic of Bulgaria is a party;

7. provide general direction of the activities relating to the background investigation of the persons who require to operate with classified information, and relating to the issuance of the appropriate levels of clearance for access to classified information ("clearance");

8. provide general direction of the activities relating to the background investigation of natural or legal persons proposing to enter or performing a contract which involves access to classified information, and shall approve a sample security certificate under this Act ("certificate");

9. jointly with the security services, conduct background investigations of, and subject to the advice of such services, issue clearance to, personsnominated for appointment as information security officers;

10. issue documents certifying to such foreign authorities as it may concern that Bulgarian natural or

legal persons have been issued with clearance or certificate, as the case may be;

11. jointly with the security services, conduct background investigations of Bulgarian citizens who apply for a position or for the performance of a special assignment which requires such citizens to operate with the classified information of another State or of an international organisation, at the written request of the competent information security authority of such State or international organisation;

12. maintain single registers of clearances, certificates, certifying or confirming documents issued, revoked or terminated, and of refusals to issue or terminate such papers, and a register of the materials and documents which contain classified information, such information being a State secret or an official secret;

13. advise immediately the Prime Minister in the event of unauthorised access to information classified as "Top Secret";

14. organise and coordinate the training for operation with classified information;

15. provide technical guidance to information security officers;

16. exercise general control over the protection of such classified information as is stored, processed or transmitted by automated informationsystems or networks;

17. issue visit permits to persons performing inspections in pursuance of international treaties relating to the reciprocal protection of classified information.

Article 10

(1) For the purposes of performing its functions and activities under Article 9, SISC:

1. may require information from the information bases of the security services and the public order services;

2. shall be provided, immediately upon request and free of charge, with thenecessary information by the government authorities and by the authorities of local self-government;

3. shall be provided, immediately upon request and free of charge, with thenecessary information by any natural or legal person in accordance with theexisting legislation. Such persons may refuse to provide such information as is unrelated to a background investigation to which they had consented or of which they had been properly notified;

4. shall issue mandatory instructions to the persons responsible hereunder.

(2) The conditions and procedure for the provision of information under subparagraphs 1 2 and 3 of paragraph 1 shall be laid down in the Detailed Rules for the Application hereof.

Section II

Functions of the Security Services

Article 11

(1) The security services shall have a duty to:

1. conduct background investigations of their officers and applicants for appointment, and shall issue, revoke or terminate the clearances of such officers or applicants;

2. conduct background investigations of natural or legal persons proposing to enter or performing a contract which involves access the classified information, and shall issue certificates of compliance with the security requirements hereunder;

3. provide assistance to SISC with the performance of its functions under Article 9, paragraphs 9, 10, 11, 13, 14 and 17;

4. provide assistance with the performance of the functions under paragraph2, subparagraph 3 of this Article and under Article 12(2).

(2) The National Security Service of the Ministry of Home Affairs shall, inaddition to its duties under paragraph 1, have a duty to:

1. conduct background investigations of the persons who require to operate with classified information, and shall issue, revoke, terminate or deny clearance for access, except in the circumstances under Article 22, paragraph 1, subparagraph 5;

2. issue confirming documents to foreign natural or legal persons on the basis of clearance or certificate issued by the appropriate competent authority of another State or of an international organisation and subject to a background investigation conducted in the Republic of Bulgaria ("confirmation"), except in the circumstances under paragraph 3, subparagraph 3;

3. exercise direct control over the protection of classified information and the compliance with the relevant legal provisions.

(3) Within the units of the Ministry of Defence and of the Bulgarian Armed Forces, excepting the Military Information Service, - the Military Police and Military Counterintelligence Security Service of the Minister of Defence shall, in addition to its duties under paragraph 1 and paragraph 2,subparagraph 3, have a duty to:

1. conduct background investigations and issue, revoke, and terminate the clearances of Bulgarian conscripts, enlisted or non-enlisted servicemen, reservists or civilians officially appointed to, or employed by, any unit of the Ministry of Defence or of the Bulgarian Armed Forces, or any second-tier budget obligor under the Minister of Defence;

2. conduct background investigations and issue, revoke, and terminate the clearances of natural persons or the certificates of legal persons proposing to perform or performing an activity for the Ministry of Defence or for the Bulgarian Armed Forces or for any second-tier budget obligor under the Minister of Defence;

3. issue confirmations to foreign citizens for the purposes of work and/or training at the Ministry of Defence or in the Bulgarian Armed Forces or at any second-tier budget obligor under the Minister of Defence;

(4) In pursuance of their duties under paragraphs 1, 2 and 3, the security services shall have a right to:

1. apply and make use of intelligence gathering techniques under such conditions and procedure as shall be laid down in law;

2. apply and make use of special surveillance devices under the conditions and procedure laid down in the Special Surveillance Devices Act with respect to any applicant for access to information classified as "Top Secret";

3. make use of data available in their information bases relating to any natural or legal person who is the subject of a background investigation;

4. store the data gathered in the course of the background investigation ofany natural person or any bidder, whether a natural or a legal person, for the purposes of entering or performing a contract which involves access to classified information;

5. store data relating to cases of unauthorised access to classified information;

6. the necessary information to be provided by any government authority or local self-government authority, or natural or legal person in accordance with the existing legislation. The conditions and procedure for the provision of such information shall be laid down in the Detailed Rules for the Application hereof.

(5) In pursuance of their duties under paragraphs 1-4, the security services shall collaborate with one another.

Article 12

For the purposes of exercising direct control over the protection of classified information and the compliance with the relevant legal provisions, the head of the National Security Service and the head of the Military Police and Military Counterintelligence Security Service shall issue an order in writing to designate officers who shall have a right to:

1. access to the sites and premises of the controlled organisational units,including the right to perform physical inspections of such sites and premises;

2. access to the documents relating to the arrangements made for the protection of classified information at the controlled organisational units;

3. access to the automated information systems or networks used for the generation, the storing, the processing or the transmission of classified information, with a view to establishing the security level of such systemsor networks;

4. where necessary, require written or oral explanations from the heads or the officers of the controlled organisational units;

5. for the purposes of an inspection at a controlled organisational unit, require information from other organisational units and, where necessary, explanations from the heads or officers thereof, relating to the generation, the processing, the storing or the release of classified information;

6. use experts where special expertise is necessary to establish facts and circumstances in the course of an inspection;

7. prescribe concrete measures relating to the protection of classified information.

Article 13

The procedure for the inspections under Article 12 shall be laid down in a Regulation by the Council of Ministers.

Article 14

The Communication Devices Protection Directorate of the Ministry of Home Affairs shall have a duty to:

1. perform the activities relating to the cryptographic protection of classified information in pursuance of Article 124 of the Ministry of Home Affairs Act;

2. issue security compliance certificates of automated information systems or networks used for operation with classified information;

3. coordinate and control the electromagnetic interference countermeasures protecting the technical devices used to process, store or transmit classified information;

4. provide and control the training of persons cleared for access to classified information in the use of cryptographic methods and devices.

Section III

Public Order Services

Article 15

The public order services shall conduct background investigations of their officers and applicants for appointment, and shall issue, revoke or terminate the clearances thereof.

Article 16

(1) In pursuance of their duties under Article 15, the public order services shall have a right to:

1. apply and make use of operational search techniques and devices under such conditions and procedure as shall be laid down in law;

2. make use of data available in their information bases relating to any natural or legal person who is the subject of a background investigation;

3. store the data gathered in the course of the background investigation oftheir officers;

4. store data relating to cases of unauthorised access to classified information by the officers under Article 15;

5. the necessary information to be provided by other organisational units in connection with a background investigation under Article 15.

(2) The public order services shall, within the limits of their duties and powers, provide assistance to the security services in connection with the pursuance of their duties under Article 11.

Section IV

Duties of Organisational Units

Article 17

The organisational units shall have a duty to:

1. apply the requirements relating to the protection of classified information and control compliance therewith;

2. be responsible for the protection of information;

3. in the event of unauthorised access to classified information, advise immediately SISC and take action to limit the harmful consequences;

4. provide the information under Article 10(1), subparagraph 2, Article 11(4), subparagraph 6, and Article 16(1), subparagraph 5.

Article 18

(1) The officers of organisational units cleared for access to a particularlevel of classified information shall have a duty to:

1. protect such classified information from unauthorised access;

2. advise immediately the information security officer in the event of unauthorised access to classified information;

3. advise the information security officer of all modifications to classified materials and documents where unauthorised access is not the case;

4. undergo medical examinations from time to time, but not less frequently than once in every two

years, and psychological tests under the conditions and procedure laid down in Article 42(3).

(2) Every person cleared for access to information classified as "Top Secret" shall have a duty to notify the information security officer of every intended private foreign travel prior to the date of departure, except where such travel is to any State with which the Republic of Bulgaria has concluded a treaty on the reciprocal protection of classified information.

(3) The provisions of paragraph 2 shall not apply to the persons under Article 39(1).

The officers of the security services and the public order services shall notify in writing their superiors of every intended foreign travel.

(4) The servicemen and the civilian personnel of the Ministry of Defence and of the Bulgarian Armed Forces shall notify in writing the head of the Military Police and Military Counterintelligence Security Service of every intended foreign travel.

Article 19

Every person cleared for access to classified information in connection with a special assignment shall have a duty to comply with the conditions and procedure for the protection of classified information.

Section V

Information Security Officer

Article 20

(1) The head of each organisational unit shall direct, organise and controlthe activities relating to the protection of classified information.

(2) The head of each organisational unit shall appoint an information security officer subject to that person being cleared by SISC for access toclassified information.

(3) By way of an exception, depending on the level and volume of classifiedinformation, the head of an organisational unit may perform the functions of information security officer, provided that he shall meet the requirements under Article 21.

(4) The information security officer shall report directly to the head of the organisational unit.

Article 21

(1) No person may be appointed information security officer unless he meetsthe following requirements:

1. such person is a Bulgarian citizen and not simultaneously the citizen ofany other State; and

2. has been cleared for access to the appropriate level of classified information under the conditions and procedure laid down in Chapter Five.

(2) Upon his appointment, the information security officer shall undergo training in the protection of classified information.

Article 22

(1) The information security officer shall have a duty to:

1. ensure compliance with the provisions of this Act and of the international treaties relating to the protection of classified information;

2. apply the rules relating to the types of classified information protection;

3. develop a security plan for the organisational unit, providing for physical and technical security

measures, and ensure its implementation;

4. inspect from time to time the records and the flow of materials and documents;

5. conduct ordinary background investigation under Article 47;

6. administer the procedure for ordinary background investigation within the organisational unit and maintain a register of persons so investigated;

7. advise SISC accordingly upon the expiration of clearances, the termination or relocation of officers, or, as the case may be, of the need to modify a clearance for access to a particular level of classified information;

8. advise, immediately and in writing, SISC and the appropriate service of any change of circumstances relating to clearances, certificates, certifying documents or confirmations issued;

9. maintain a record of the cases of unauthorised access to classified information and of actions taken, and advise SISC immediately of each such case and action;

10. ensure the classification of information at the appropriate level;

11. develop a plan for the protection of classified information during a state of war, martial law or any other state of emergency;

12. organise and administer the training of the organisational unit officers in the protection of classified information.

(2) Upon the occurrence of circumstances under paragraph 1, subparagraph 7, 8 or 9, the information security officers of the security or the public order services shall immediately advise the respective head of service.

(3) The information security officers of the Ministry of Defence and of theBulgarian Armed Forces shall, upon the occurrence of circumstances under paragraph 1, subparagraph 8 or 9, immediately advise the Military Police and Military Counterintelligence Security Service.

Section VI

Administrative Units for Information Security

Article 23

In pursuance of his duties under Article 22, and depending on the volume ofclassified information, the information security officer may be supported by an administrative unit for information security.

Article 24

No person may be appointed to any unit under Article 23 unless he meets therequirements under Article 21.

Chapter Three

CLASSES OF CLASSIFIED INFORMATION AND

CLASSIFICATION LEVELS

Section I

Classified Information

Article 25

State secret is such information, as listed in Schedule 1, the unauthorisedaccess to which might threaten

or prejudice such interests of the Republic of Bulgaria as relate to national security, defence, foreign policy or the protection of the constitutional order.

Article 26

(1) Official secret is such information as is generated or stored by government authorities or by the authorities of local self government, is not a State secret, and the unauthorised access to which might adversely affect the interests of the State or prejudice another interest protected by law.

(2) The information which shall be the subject of classification as an official secret shall be determined by law.

(3) The heads of organisational units shall, within the limits hereunder, announce a list of the classes of information under paragraph 2 within their respective field of activity. The procedure for, and the manner of, such announcement shall be laid down in the Detailed Rules for the Application hereof.

Article 27

Foreign classified information is such classified information as has been disclosed by another State or by an international organisation in pursuanceof an international treaty to which the Republic of Bulgaria is a party.

Section II

Classification Levels

Article 28

(1) The information classification levels and their respective wordings shall be the following:

1. "Top Secret";

2. "Secret";

3. "Confidential";

4. "Four Official Use Only".

(2) The information which is a State secret shall be marked for security level as follows:

1. where the unauthorised access to such information might pose an exceptionally high threat to the sovereignty, the independence or the territorial integrity of the Republic of Bulgaria, or to its foreign policyor international relations in the field of national security, or might posea threat of irreparable or exceptionally grave damage, or cause such damagein the field of national security, defence, foreign policy or the protection of the constitutional order, - "Top Secret";

2. where unauthorised access to such information might pose a high threat to the sovereignty, the independence or the territorial integrity of the Republic of Bulgaria, or to its foreign policy or international relations in the field of national security, or might pose a threat of nearly irreparable or grave damage, or cause such damage in the field of national security, defence, foreign policy or the protection of the constitutional order, - "Secret";

3. where unauthorised access to such information might pose a threat to thesovereignty, the independence or the territorial integrity of the Republic of Bulgaria, or to its foreign policy or international relations in the field of national security, or might pose a threat of damage, or cause damage in the field of national security, defence, foreign policy or the protection of the constitutional order, -"Confidential".

(3) The information classified as an official secret shall be marked "Four Official Use Only".

(4) With a view to ensuring a higher level of protection, as necessary having regard to the character of the subject information or the provisionsof international treaties to which the Republic of Bulgaria is a party, SISC may by its decision, subject to the advice of the Minister of Home Affairs or the Minister of Defence or any of the directors of the security services, prescribe:

1. additional markings for materials and documents classified higher than "Top Secret";

2. a special procedure for the generation, use, reproduction, release, and storage of such materials and documents;

3. the categories of persons cleared for access to such materials and documents.

Article 29

The classification levels of foreign classified information received by theRepublic of Bulgaria from, or of classified information disclosed by the Republic of Bulgaria to, another State or an international organisation, inpursuance of an international treaty which has come into force for the Republic of Bulgaria and for that other State or international organisation, shall be aligned in accordance with such treaty.

Chapter Four

MARKING OF INFORMATION

Section I

Marking Procedure of Classified Information

Article 30

(1) Classified information shall be identified by an appropriate security marking.

(2) Such security marking shall contain:

1. Classification level.

2. Date of classification.

3. Date on which the classification period shall expire, where such date isdifferent from the date on which the appropriate period under Article 34(1)shall expire.

4. Legal reasons for classification.

(3) A compilation of materials and/or documents which are individually identified by different security markings shall be identified in its entirety by the appropriate security marking of that material or document contained in the compilation which is classified at the highest level.

Article 31

(1) The appropriate security marking shall be determined by the authorised signer of the document which contains classified information or certifies the existence of classified information in a material other than that document.

(2) The person who has generated a document or material containing classified information, where such person is other than the person under paragraph 1, shall identify such document by an appropriate security marking which shall be valid until the final determination of the security marking by the person under paragraph 1.

(3) The persons who have a duty to mark classified information shall be responsible for marking or the omission to mark such information.

(4) The making, the modification or the deletion of a security marking shall not be allowed outside the clearance limits of the person who makes or modifies or deletes such marking.

(5) Classified information may not be identified by any security marking other than the one appropriate to the classification level as determined inpursuance of this Act and the Detailed Rules for the Application hereof.

(6) The level at which information is classified may not be modified or removed without the consent of the person under paragraph 1 or of such person's superior.

(7) The level at which information is classified may not be modified without a valid reason.

(8) Whoever, having lawfully received classified information, finds that such information has been classified at other than the appropriate level shall immediately advise the person under paragraph 1 or such person's superior.

(9) If the person so advised chooses to modify the level at which the information is classified, he shall immediately advise the recipient thereof. Upon submission of classified information to third parties the recipient shall immediately advise those parties on the modification.

(10) The heads of organisational units shall organise the training of theirofficers in the conditions and procedure for the security marking of information (the making, modification, and deletion of security markings) under the technical guidance of SISC.

Article 32

The procedure for, and the manner of, the security marking of information shall be laid down in the Detailed Rules for the Application hereof.

Section II

Storing of Classified Information

Article 33

(1) Classified information shall be generated, processed, released, stored,and destroyed under the conditions and procedure laid down in this Act and in the implementing statutory instruments hereto, and in accordance with the types of protection provided for, and corresponding to, the classification level, except as otherwise may be provided in an international treaty to which the Republic of Bulgaria is a party.

(2) Within one year from the expiration of the protection period, the information shall be transferred to the State Archives, except as otherwisemay be provided by a special legislative instrument.

(3) Information may not be destroyed until one year after the expiration ofthe protection period.

(4) The State Information Security Commission shall authorise information to be destroyed, subject to the advice of a committee instituted by the order of the head of the appropriate organisational unit. Such committee shall:

1. give an opinion as to which information is of no historical, practical or a referential importance;

2. give an advice to destroy documents and materials.

(5) The SISC decision to destroy information shall be appealable before theSupreme Administrative Court.

Section III

Protection Periods of Classified Information

Article 34

(1) The following shall be the protection periods of classified information, to commence from the date of generation:

1. of information marked as "Top Secret", 30 years;

2. of information marked as "Secret", 15 years;

3. of information marked as "Confidential", five years;

4. of information classified as an official secret, two years.

(2) Where national interest so requires, SISC may decide to extend the periods under paragraph 1, provided however that the extension shall not exceed the original protection period.

(3) Upon the expiration of the periods under paragraphs 1 and 2, the subject information shall be declassified and the access to such information shall be governed by the Access to Public Information Act.

(4) Where an organisational unit is completely abolished, its classified information whish is a State secret or an official secret, and all its powers to modify the classification levels thereof, shall be transferred toSISC, except as otherwise may be provided by a special legislative instrument.

(5) The periods under paragraphs 1 and 2 shall apply as well to foreign classified information, except as otherwise may be provided by an international treaty to which the Republic of Bulgaria is a party.

Article 35

(1) The State Information Security Commission shall maintain a register of the materials and documents which contain classified information which is aState secret or an official secret.

(2) The register under paragraph 1 shall contain the following elements:

1. Organisational unit which generated the material or document.

2. Generation date and declassification date.

3. Identification number of the material or document under which it is entered on the register under paragraph 1.

4. Legal reasons for the classification of the material or document, and its security marking.

5. Modification of the classification level or declassification, and the date thereof.

(3) Upon generation of a material or document which contains classified information which is a State secret or an official secret, or upon modification of the classification level or the declassification thereof, as the case may be, the heads of organisational units shall provide the elements under paragraph 2, subparagraphs 1, 2, 4, and 5, to SISC for entryon the register.

(4) The persons under Article 31(1) shall, from time to time, but not less frequently than once in every two years, revue the protection period of each material or document having a security marking for the existence of any legal reasons to modify its classification level or to declassify such material or document. In the event of modification of the classification level, the portion of the protection period under Article 34(1) prior to such modification shall be subtracted from the protection period corresponding to the new classification level.

(5) The procedure for the provision of the registration elements, and the conditions and procedure for retrieving information from the register, shall be laid down in the Detailed Rules for the Application hereof.

Chapter Five

ACCESS TO CLASSIFIED INFORMATION

Section I

Conditions for Access

Article 36

Except in the circumstances under Article 39, no person shall have a right of access to classified information merely by reason of official status.

Article 37

(1) The heads of organisational units, excepting those under paragraph 2, shall establish a list of the positions and assignments, and the respectiveclassification levels, which require access to classified information whichis a State secret.

(2) The heads of the security services and the public order of services shall establish the list under paragraph 1 for their respective services.

Article 38

(1) Access to classified information in connection with the performance of official duties or special assignments may not be allowed prior to:

1. the completion of a background investigation of the person to be allowedsuch access; and

2. the training of such person in the protection of classified information.

(2) No background investigation shall be conducted for the purposes of information classified as an official secret.

Article 39

(1) No background investigation shall be conducted of the following persons:

1. the Speaker of the National Assembly;

2. the President of the Republic of Bulgaria;

3. the Prime Minister;

4. the Government Ministers;

5. the Chief Clerk of the Council of Ministers;

6. the Members of the National Assembly;

7. (Supplemented, SG No. 55/2004) the Justices of the Constitutional Court,the Judges, the Prosecutors, the Lawyers and the Investigators.

(2) The persons under paragraph 1, subparagraphs 1, 2 and 3, shall, effective from the assumption of office, have a right of access to all levels of classified information for the duration of their term in office.

(3) The persons under paragraph 1, subparagraphs 4, 5, 6 and 7, shall, effective from the assumption of office, have a right of access to all levels of classified information for the duration of their term in office in keeping with the "need-to-know" principle and, where the subject information is:

1. for the Government Ministers and the Chief Clerk of the Council of Ministers, within their respective terms of reference;

2. for the Members of the National Assembly, subject to a decision, properly made, of a Parliamentary Committee or of the Assembly, or providedthat such Committee or the Assembly meets in a closed session;

3. (Supplemented, SG No. 52/2004) for the Judges, Prosecutors, Lawyers and Investigators, for the purposes only of the case at hand.

Article 39a

(New, SG No. 89/2004)

(1) No reliability clearance shall be carried out in respect of persons upon or in relation to the exercise of their constitutional right to defence.

(2) Persons under para 1 shall ex lege have access to all levels of classified information for the time required for the exercise of their right to defence and in compliance with the "need to know" principle.

Article 40

(1) In no circumstance other than the ones under Article 39, shall a clearance for access to classified information be issued to any person, unless he meets the following requirements:

1. such person is a Bulgarian citizen, except in the circumstances under Chapter Six, Section VI; and

2. is of legal age; and

3. has completed secondary education; and

4. has not been convicted of premeditated felony, subsequent rehabilitationnotwithstanding; and

5. is not the subject of any pre-trial or trial proceeding for premeditatedfelony; and

6. is reliable for the purposes of security; and

7. is not suffering from any mental disorder, as duly certified; and

8. is considered reliable for the purpose of protecting a secret.

(2) Where an international treaty exists to which the Republic of Bulgaria is a party, or on the basis of reciprocity, the requirements under paragraph 1 shall not apply to citizens of other States who, in the Republic of Bulgaria, perform such tasks as may be assigned to them by the State concerned or by an international organisation, provided that such persons shall have been cleared for access to classified information by theappropriate information security authority of such State or international organisation.

Article 41

A person shall be deemed to be reliable for the purposes of security in theabsence of any data implicating such person:

1. in any activity directed against the interests of the Republic of Bulgaria or against any interest which the Republic of Bulgaria has undertaken to safeguard in pursuance of international treaties;

2. as a participant in, or an accomplice to, any espionage, terrorist, sabotage or subversive activity;

3. in any other activity directed against the national security, the territorial integrity or the sovereignty of the Republic of Bulgaria or aimed at changing the constitutional order by the use of violence;

4. in any activity directed against public order.

Article 42

(1) A person shall be deemed reliable for the purpose of protecting a secret in the absence of any data to evidence:

1. any concealment of information or misrepresentation by such person for the purposes of the background investigation;

2. any facts or circumstances which might render such person vulnerable to blackmail;

3. a discrepancy between such person's living standard and his income;

4. a mental disorder or any other psychic disorder which might impair such person's capacity to operate with classified information;

5. such person's addiction to alcohol or psychotropic substances.

(2) For the purpose of establishing the facts under paragraph 1, subparagraphs 4 and 5, the investigating authority may require the person under investigation to undergo special medical and psychological tests and to present the results thereof. The person under investigation may refuse to undergo such tests. Such refusal shall be made in writing, and the background investigation shall be terminated.

(3) The procedure for, and the places of, the above special medical and psychological tests, as well as the periodical medical examinations under Article 18(1), subparagraph 4, and the methods thereof, shall be prescribed in a regulation by the Minister of Health, subject to consultation with SISC.

Section II

Background Investigation Procedure

Article 43

(1) The background investigation procedure shall have the purpose of establishing whether an applicant meets the requirements for clearance for access to classified information.

(2) The background investigation procedure shall be conducted subject to the written consent of the person concerned.

(3) All such investigation activities shall be documented.

(4) The written consent under paragraph 2 may be withdrawn at any time during the investigation.

(5) In the event of such withdrawal, the person concerned shall not have a right to apply for appointment or for the performance of a special assignment, which requires access to classified information, for a period of one year thereafter.

(6) In the circumstances under paragraph 4, the background investigation procedure shall be terminated immediately. Any materials or documents produced by the person under investigation shall be returned to him, and the data gathered in the course of the investigation shall be destroyed immediately by the investigating authority.

(7) The procedure for the purposes of paragraph 6 shall be laid down in theDetailed Rules for the Application hereof.

Article 44

(1) With a view to establishing the reliability of a person under background investigation for the purpose of protecting a secret, data shallbe gathered in the course of such investigation about such third parties asthe person under investigation shall specify in the appropriate questionnaire.

(2) The processing of personal data for the purposes of paragraph 1 shall be governed by the Personal Data Protection Act.

Article 45

(1) The investigation under Article 43(1) shall be conducted for first applicants for the positions or assignments described in pursuance of Article 37.

(2) The investigation under paragraph 1 shall be conducted also for personswhose work requires access to information classified at a higher level.

(3) The applicants in a competitive examination procedure for appointment or for the performance of a special assignment which requires access to classified information must meet the requirements hereunder for clearance for access to the appropriate level of classified information.

(4) The requirement under paragraph 3 shall be expressly cited in the announcement of the competitive examination.

(5) The specific requirements relating to the conduct of the investigation procedure for the persons under paragraph 3 shall be laid down in the Detailed Rules for the Application hereof.

Section III

Types of Background Investigation

Article 46

The following types of background investigation shall be conducted depending on the level of clearance required:

1. ordinary investigation, for access to information classified as "Confidential";

2. extensive investigation, for access to information classified as "Secret";

3. special investigation, for access to information classified as "Top Secret".

Article 47

(1) Ordinary investigation shall be conducted by the information security officer upon the written instructions of the head of the organisational unit.

(2) In the circumstances under Article 20 (3), such investigation shall be conducted by the head of the organisational unit.

(3) Ordinary investigation shall be conducted for the purpose of establishing the facts and circumstances under Article 40 (1), paragraphs 1 - 5, 7 and 8.

(4) The investigation under paragraph 1 shall include the completion of a questionnaire (Schedule 2).

(5) To verify the facts and circumstances under paragraph 4, the information security officer shall have a right to require and to receive data from the public order services and from the competent government authorities, and, as necessary, shall have a right to require assistance from the security services.

(6) The information security officer shall conclude the investigation and shall issue or deny clearance for access to information which is a State secret and is classified as "Confidential", and shall promptly advise SISC.

Article 48

(1) Extensive investigation shall be conducted for persons who apply for appointment or for the performance of a special assignment which requires operation with information classified as "Secret".

(2) The investigation under paragraph 1 shall be conducted, except in the circumstances under Articles 11 and 15, by the National Security Service atthe written request of the head of the organisational unit to which the person concerned applies for appointment or which issues a special assignment.

(3) The investigation under paragraph 1 shall be conducted for the purpose of establishing the facts and circumstances under Article 40(1).

(4) The investigation under paragraph 1 shall include the completion of a questionnaire (Schedule 2).

(5) (Amended, SG No. 31/2003) The extensive investigation shall, in addition to establishing and verifying the facts and circumstances under paragraphs 3 and 4, include verifications at the domicile and the place of work, and of the bank accounts of the person under investigation, and in the tax registers, and from the Financial Intelligence Agency.

Article 49

(1) Special investigation shall be conducted for persons who apply for appointment or for the performance of a special assignment which requires operation with information classified as "Top Secret".

(2) The investigation under paragraph 1 shall be conducted, except in the circumstances under Articles 11 and 15, by the National Security Service atthe written request of the head of the organisational unit to which the person concerned applies for appointment or which issues a special assignment.

(3) The special investigation shall include the activities under Article 48, paragraphs 3-5, and an interview with the person under investigation and with three other persons, such as the person under investigation shall specify.

Article 50

(1) If any facts and circumstances are revealed in the course of the examination under Articles 47, 48 or 49, such as present an impediment to the issuance of the appropriate level clearance, there shall be conducted an additional interview with the person under investigation.

(2) The interview under paragraph 1 shall be conducted for the purpose of obtaining greater clarity on the facts and circumstances so revealed.

(3) Such interview shall be conducted, depending on the type of investigation under way, by:

1. where an ordinary investigation, the information security officer or, asthe case may be under Article 20(3), the head of the organisational unit;

2. where an extensive or a special investigation, the appropriate investigating authority.

(4) No interview under paragraph 1 shall be conducted where, were it to be conducted, such interview might entail an unauthorised access to information which is a State secret.

Article 51

Within the Ministry of Defence and the Bulgarian Armed Forces, the investigation under Articles 47(1), 48(1) and 49(1) shall be conducted by the authority under Article 11(3) at the written request of the head of theappropriate structural unit.

Section IV

Time Limits for Investigation and Issuance or Denial of Clearance

Article 52

(1) The background investigation shall be completed within the following time limits:

1. of an ordinary investigation, 30 days from the date of receipt of the relevant instructions or request;

2. of an extensive investigation, 45 days from the date of receipt of the relevant written request of the head of the organisational unit;

3. of a special investigation, 60 days from the date of receipt of the relevant written request of the head of the organisational unit.

(2) The appropriate heads of units may extend the time limits under paragraph 1, but by not more than 20 days, on the basis of the written reasoned request of the officers of the security or the public order services, or of the information security officers, conducting the investigation, provided however that such request shall be made prior to the expiration of the original time limit.

Article 53

The State Information Security Commission, the services under Articles 11 and 15 or the information security officer shall issue or deny clearance for access to information classified at the appropriate level within 10 days from the date of completion of the background investigation.

Section V

Issuance, Revocation, Termination, and Denial of Clearance

for Access the Classified Information

Article 54

(1) Clearance for access shall be issued to such persons as meet the requirements under Article 40(1) for the appropriate classification level.

(2) The clearance for access is a document made in writing. Its shall be issued in triplicate, on such sample form as SISC shall approve, to be kept, one each, by SISC, the issuing service, and the appropriate organisational unit.

(3) The clearance for access to any higher classification level shall entitle the holder thereof to access to information classified at a lower level if the latter is required by the holder's official position or performance of a special assignment.

Article 55

(1) Clearance for access shall be issued for a period of:

1. five years, to information classified as "Confidential";

2. four years, to information classified as "Secret";

3. three years, to information classified as "Top Secret".

(2) Not later than three months before the expiration of a period under paragraph 1, a new background investigation shall be conducted of the persons who continue in a position, or with the performance of a special assignment, which requires access to information classified at the appropriate level.

(3) The investigation under paragraph 2 and the issuance of a new clearanceshall be done by the competent authorities under the conditions and procedure provided for in this Chapter.

Article 56

(1) Where, concerning a person cleared for access to classified information, new facts and circumstances are revealed which raise a doubt as to such person's reliability, the security information officer shall inquire into such facts and circumstances.

(2) The inquiry under paragraph 1 shall be conducted immediately and for the purpose of obtaining greater clarity on the said facts and circumstances.

(3) The security information officer shall advise such inquiry in writing to the head of the organisational unit and the authority which issued the clearance.

(4) Upon such advice, the head of the organisational unit may restrict the access of the person under inquiry to the appropriate classification level and shall immediately advise the issuing authority.

Article 57

(1) Clearance for access to classified information of the appropriate levelshall be denied where it is established, in the course of a background investigation, that:

1. the person under investigation does not meet any one of the requirementsunder Article 40(1);

2. the person under investigation has deliberately misrepresented or withheld any facts and circumstances.

(2) The denial of clearance shall be issued in triplicate, on such sample form as SISC shall approve, to be kept, one each, by SISC, the issuing authority, and the appropriate organisational unit.

(3) The denial of clearance shall not be accompanied with an explanation ofreasons and shall only set out the legal reasons for denial.

(4) The person under investigation shall be notified of such denial in writing, setting out the legal reasons for denial, and shall be issued witha transcript thereof.

(5) Denial of access to classified information shall not be appealable before courts of law.

(6) No person under investigation who is denied clearance for access to classified information shall have a right to apply for appointment or for the performance of a special assignment, such as requires access to information classified at the same or at a higher level, for a period of one year from the date of such denial.

Article 58

The clearance, and the denial of clearance, for access to classified information shall set out:

1. The issuing authority.

2. The full name, the date and place of birth, and the Personal Identity Number of the person under investigation.

3. The organisational unit to which such person is applying for appointment, or at which such person is working or performing a special assignment, as the case may be.

4. The type of investigation.

5. The level of classification to which access is cleared or denied.

6. The legal reasons for clearance or the denial thereof.

7. The document's term of validity.

8. The document's number.

9. The document's date and place of issuance.

10. Signature and stamp.

Article 59

(1) The issuing authority of a clearance for access to classified information shall revoke such clearance, subject to the advice, made in writing, of the appropriate information security officer, where:

1. it is established by the inquiry under Article 56 that the person concerned does not meet any one of the requirements under Article 40(1);

2. the person concerned has committed an offence under any of the provisions of this Act or of the implementing statutory instruments hereto,and has thereby threatened or caused grave damage to the interests of the State or of the organisations or persons concerned with the protection of classified information;

3. the person concerned has committed systematic offences under this Act orany statutory instrument relating to the protection of classified information.

(2) The authority under paragraph 1 shall immediately advise the revocationof clearance in writing to the appropriate head of organisational unit and to the person concerned.

(3) The revocation of clearance shall not be accompanied with an explanation of reasons and shall only set out the legal reasons for revocation.

(4) The revocation of clearance shall be based on a written statement containing the appropriate elements under Article 58.

(5) The revocation of clearance shall not be appealable before the courts of law.

(6) No person whose clearance for access to classified information is revoked shall have a right to apply for appointment or for the performance of a special assignment, such as requires access to classified information,for a period of three years from the date of such revocation.

Article 60

(1) The issuing authority of a clearance for access to classified information shall terminate such clearance, subject to the advice, made in writing, of the appropriate information security officer, in the event of:

1. the death of the holder of such clearance;

2. failure to assume, or removal from, the appropriate position;

3. termination of the performance of the appropriate special assignment;

4. expiration of the appropriate period under Article 55(1);

5. change in the need for access to information classified at a higher level.

(2) The authority under paragraph 1 shall advise the termination of clearance in writing to the appropriate head of organisational unit and to the person concerned.

(3) The termination of clearance shall not be accompanied with an explanation of reasons and shall only set out the legal reasons for termination.

(4) The termination of clearance shall be based on a written statement containing the appropriate elements under Article 58.

(5) The termination of clearance shall not be appealable before the courts of law.

Article 61

In the circumstances under Articles 59 or 60, the officer concerned shall return the clearance to the issuing authority.

Article 62

A denial of clearance for access to classified information, and the termination or revocation thereof, may be appealed before SISC within sevendays from the date of advice to the person concerned under Article 57(4) or 59(2) or 60(2), as the case may be.

Article 63

(1) Such appeal shall be made in writing and addressed to SISC in the care of the authority whose act is the subject thereof.

(2) The appeal shall set out the authority before which it is laid; the name and address of the appellant; the act which is the subject of appeal; the authority which issued such act; the appellant's complaint and petition.

Article 64

(1) Any appeal laid after the period under Article 62 shall be returned to the appellant against his acknowledgement of receipt.

(2) Within seven days of return, a request may be made for renewal of the period for appeal, provided that the original period was not complied with on account of special unforeseen circumstances. The original appeal so returned shall be attached to such request.

(3) The request for renewal of the period for appeal shall be considered by SISC. If such request is deemed to be valid, the appeal shall be admitted, and if not, the appeal shall be dismissed without a hearing.

Article 65

(1) Within seven days from the date of receipt of an appeal, the authority which issued the subject act may reconsider the matter and may issue clearance for access to classified information or, as the case may be, withdraw the act whereby clearance had been revoked. The person concerned shall be advised accordingly.

(2) If the authority which issued the subject act does not find any reason to reverse its decision, it shall immediately refer the appeal, together with all the relevant documents, to SISC.

(3) If, within seven days from the expiration of the time limit under paragraph 1, the appeal has not been referred to SISC, the appellant may send a transcript thereof to SISC or advise SISC of the delay. SISC shall require delivery of the relevant documents ex officio.

(4) After receipt of the relevant documents, SISC may gather new evidence.

Article 66

(1) The State Information Security Commission shall adjudicate on the appeal within two weeks from the date of receipt thereof.

(2) The State Information Security Commission shall adjudicate by a ruling whereby it shall revoke the administrative act of denial, termination or revocation of clearance, as the case may be, or dismiss the appeal.

(3) Where the authority concerned had unlawfully denied clearance for access to classified information, SISC may direct the authority to commencea background investigation procedure, to be completed within such time as SISC shall prescribe.

Article 67

Within three days from the date of the ruling, SISC shall announce it to the appellant, to the authority which issued the subject act, and to the appropriate organisational unit.

Article 68

The SISC ruling shall be final and shall not be subject to any further appeal.

Article 69

A denial or termination or revocation of clearance for access to classifiedinformation issued by SISC shall not be subject to appeal.

Section VI

Background Investigation Files

Article 70

(1) The files of materials relating to background investigations shall be kept, maintained, updated, card-filed, and closed by the investigating authority, separately from other files.

(2) Such file shall be opened by the competent authority upon the commencement of a background investigation.

(3) The data contained in such file is an official secret and may only be used for the purposes of this Act.

(4) The files of persons who have been cleared for access to classified information shall be kept for a period not to exceed five years after the expiration of the clearance period, whereafter, such files shall be destroyed.

Article 71

(1) The file of a person under investigation shall contain:

1. The application for appointment or the documents relating to a special assignment, which requires access to classified information, or as the casemay be, the application for a competitive examination for the purposes of such appointment or special assignment.

2. The documents relating to a natural or legal person proposing to enter or perform a contract involving access to classified information.

3. The person's written consent to the background investigation.

4. The written request for background investigation.

5. The completed investigation questionnaire.

6. The clearance, certificate, or certifying document for access to classified information.

7. The document of denial, revocation, or termination of the clearance for access to classified information.

8. The documents of appointment or special assignment.

9. The documents relating to the completion of training in the protection of classified information.

10. Any other documents evidencing facts and circumstances established in pursuance of this Act.

(2) The special rules for the opening, the storing, the maintenance, the updating, the card-filing, and the closing of background investigation files shall be laid down in the Detailed Rules for the Application hereof.

Chapter Six

TYPES OF CLASSIFIED INFORMATION PROTECTION

Section I

Physical Security

Article 72

(1) The physical security of classified information includes a system of organisational, physical, and technical measures for the prevention of unauthorised access to materials, documents, equipment, and facilities classified as a State secret or an official secret.

(2) The system of measures under paragraph 1 includes the protection of thebuildings, the premises, and facilities within or at which classified information is generated, processed, or stored, and the control of access to such buildings, premises, and facilities.

Article 73

(1) The organisational units shall apply a system of measures and devices for the physical security of the buildings, the premises, or the facilitieswithin or at which classified information is generated, processed, or stored.

(2) Physical security shall be used for the protection of classified information from any threat or damage resulting from:

1. terrorist activities or sabotage; or

2. unauthorised access or attempted unauthorised access.

(3) The necessary techniques and devices for physical security shall be determined in accordance with the classification level and the volume of classified information, the number and the clearance levels of staff, as determined pursuant to Article 3, and the level of threat of any damaging action.

Article 74

To prevent unauthorised access to classified information, the heads of organisational units, with the assistance of the information security officer, shall:

1. define security perimeters;

2. around the security perimeters, define administrative perimeters of the lowest security level within which persons and vehicles shall be controlled;

3. introduce a control arrangement for entry into, movement within, and exit from, the security perimeters, and for the escorting within such perimeters of the visitors not cleared for access to classified informationor cleared for access to information classified at a lower level than the one held within the security perimeter;

4. provide the appropriate control of the security and the administrative perimeters with the support of the appropriate security units;

5. introduce a special arrangement for the safekeeping of keys to the premises, safes and other facilities used for storing classified information.

Article 75

To protect classified information which is a State secret in the course of meetings, talks, conferences, etc, of which such information is the subject, additional security measures shall be introduced to prevent bugging or unauthorised observation.

Article 76

The persons participating in meetings or conferences, of which classified information which is a State secret is the subject, shall undergo a prior security check by the security unit of the organisational unit.

Article 77

(1) All materials and technical devices used for the protection of classified information must conform to the durability and indestructibilityrequirements appropriate to each classification level, as certified by SISCor by another authority designated by the Council of Ministers.

(2) Any technical devices other than the above may not be used otherwise than by way of an exception and provided that the appropriate security level shall not be compromised.

(3) The physical security measures, as certified for each classification level, shall be described in a schedule which SISC shall approve.

Article 78

The system of physical security measures, techniques, and devices, and the conditions and procedure for the operation thereof, shall be laid down in aregulation by the Council of Ministers.

Article 79

The information security officers shall exercise ex ante and current control over the physical security arrangements, techniques, and devices attheir respective organisational unit.

Section II

Documentary Security

Article 80

(1) Documentary security is a system of measures, techniques, and devices for the protection of classified information during the preparation, the processing, and the storing of documents, and in the organisation and operation of classified information registries.

(2) The system of documentary protection measures, techniques, and devices,and the conditions and procedure for the operation thereof, shall be laid down in the Detailed Rules for the Application hereof.

Article 81

To ensure the protection of classified information, the heads of organisational units shall, within their terms of reference, establish additional special procedures and requirements.

Article 82

(1) Within each organisational unit, their shall be created a separate classified information registry which shall be responsible for the proper preparation, processing, and storing, and delivery to the authorised persons of materials which contain classified information. Such classified information registry shall report directly to the appropriate information security officer.

(2) Requirements relating to the organisation and operation of the registries under paragraph 1 shall be laid down in the Detailed Rules for the Application hereof.

Section III

Personal Security

Article 83

(1) Personal security is a system of such principles and measures as the competent authorities,

following the appropriate procedure, shall apply to persons with a view to ensuring such persons' reliability for the purposes of protecting classified information.

(2) The principles and measures under paragraph 1 include the "need to- know" principle, the background investigation procedure, and the issuance of access clearance under Chapter Five, the training of persons pursuant to this Act and the Detailed Rules for the Application hereof, andthe exercise of control in these areas.

Section IV

Cryptographic Security

Article 84

Cryptographic security is a system of cryptographic methods and devices used to protect classified information from unauthorised access during the generation, the processing, the storing, and the transmission of such information.

Article 85

The conditions and procedure for the manufacture and import of cryptographic methods and devices for the protection of classified information shall be laid down in a regulation by the Council of Ministers,subject to the advice of the Minister of Home Affairs.

Article 86

No cryptographic method or device shall be used for the protection of classified information prior to the approval and registration of such method or device by the Communication Devices Protection Directorate of theMinistry of Home Affairs.

Article 87

(1) The generation and distribution of the necessary cryptographic keys shall be the responsibility of the Communication Devices Protection Directorate of the Ministry of Home Affairs.

(2) The activities under paragraph 1 may be performed as well by any other organisational unit, subject to the prior approval, and under the control of the Communication Devices Protection Directorate of the Ministry of HomeAffairs.

Article 88

(1) Within each organisational unit, the use of cryptographic methods and devices shall be the responsibility of the information security officer, orof such other officers of the administrative security unit who have been trained in the field of cryptographic security and have been authorised to use cryptographic devices.

(2) The authorisation under paragraph 1 shall be issued by the Communication Devices Protection Directorate of the Ministry of Home Affairs, subject to prior background investigation under Article 46(3). The issuance, termination or revocation of such authorisation shall be governed by the provisions of Chapter Five. The denial, termination or revocation of such authorisation shall not be appealable before the courts of law.

(3) The training under paragraph 1 shall be administered by the Communication Devices Protection Directorate of the Ministry of Home Affairs, or by any other organisational unit, subject to the prior approval, and under the control of the said Directorate.

Section V

Automated Information Systems Security

Article 89

The security of automated information systems (AIS) or networks is a systemof principles and measures for the protection from unauthorised access of such classified information as is generated, processed, stored, or transmitted by AIS or networks.

Article 90

(1) The general required conditions for the security of AIS or networks include computer security, communications security, cryptographic security,physical security, and personal security, the security of information as such on any electronic medium, and electromagnetic interference countermeasures, as defined in a regulation by the Council of Ministers, subject to the advice of the Minister of Home Affairs.

(2) The specific requirements for the security of AIS or networks within each organisational unit shall be defined by the head of such unit, subjectto the advice of the information security officer. These requirements shallbe adopted subject to the approval of the Communication Devices Protection Directorate of the Ministry of Home Affairs.

(3) The requirements under paragraph 2 shall include a detailed descriptionof the security measures and rules applied to the design and operation of the AIS or network.

(4) The requirements under paragraph 2 shall be defined in the design phaseof the AIS or network, and shall be modified, as necessary, in the process of deployment and development of the system.

(5) All subsequent modifications to the requirements under paragraph 2 shall be adopted subject to the approval of the Communication Devices Protection Directorate of the Ministry of Home Affairs.

Article 91

Prior to the placement of an AIS or network into service, the CommunicationDevices Protection Directorate of the Ministry of Home Affairs shall conduct a comprehensive security assessment of such AIS or network for compliance with the requirements under Article 90, and shall issue the certificate under Article 14(2) on such sample form as shall be prescribed in a regulation under Article 90(1).

Article 92

The head of an organisational unit which operates an AIS or network for theprocessing of classified information shall, subject to the advice of the information security officer, appoint or designate officers of the administrative security unit to control compliance with the security requirements for such AIS or network.

Article 93

No classified information may be generated, processed, stored, or transmitted by an AIS or network, unless such AIS or network is duly certified in pursuance of the provisions of this Section.

Article 94

No AIS or network used for the generation, the processing, the storing, or the transmission of classified information may be interconnected with any public network, such as the Internet or such other electronic communicationnetworks.

Section VI

Industrial Security

Article 95

(1) Industrial security is a system of principles and measures applied to persons, whether natural or legal, who propose to enter or perform a contract which involves access to classified information, for the purposes of protecting such information from unauthorised access.

(2) The general industrial security requirements shall be defined pursuant to this Act in a regulation by the Council of Ministers.

(3) Subject to the advice of SISC, the Council of Ministers shall designatean authority to perform background investigations and issue security certificates.

(4) The contract under paragraph 1 shall provide specific requirements for the protection of classified information, relating in particular to the volume and level of classified information, the persons allowed access thereto, and the liability for non-compliance with the industrial security requirements.

Article 96

(1) Classified information may not be disclosed to any natural person, unless such person is certified and cleared for access to such information,nor to any legal person, unless such person is certified for such access.

(2) In circumstances other than those under paragraph 1, where there are reasons to believe that, in the course of operation, a person may generate or receive access to classified information, such person shall have a duty to request clearance under Chapter Five or certificate under this Section.

Article 97

(1) For the purposes of certification, the bidder shall undergo background investigation whereby data shall be gathered about:

1. the bidder's management personnel, and the persons immediately involved in the performance of the contract under Article 95(1);

2. the persons involved in the negotiations on the contract under Article 95(1);

3. the bidder 's administrative security unit personnel.

(1) For the purposes of such background investigation, data shall be gathered also about:

1. the bidder's structure and origin of capital;

2. the bidder's commercial partners, financial relations, real rights, etc,as necessary to assess the bidder's reliability.

Article 98

(1) For the purposes of the above background investigation, the bidder shall complete a questionnaire, as defined in the Detailed Rules for the Application hereof.

(2) In the event of any subsequent change in the data entered in the questionnaire under paragraph 1, the bidder shall have a duty to advise immediately the investigating authority.

Article 99

A bidder which misrepresents data, or provides incomplete data, for the purposes of the questionnaire under Article 98(1) shall not be certified for access to classified information.

Article 100

No bidder shall be certified for access the classified information, unless such bidder:

1. meets the security requirements under this Act and the implementing statutory instruments hereto;

2. is economically stable;

3. is reliable for the purposes of security.

Article 101

(1) No bidder shall be deemed to be economically stable if such bidder:

1. has been declared bankrupt or is in pending bankruptcy proceedings;

2. has been convicted of fraudulent bankruptcy;

3. is in liquidation;

4. has been barred from carrying on commercial activities;

5. has a liability, liquid, due and payable, to the Treasury or to any social security fund or to any natural or legal person, where such liability has been accepted before the authority of writ or has been established by an effective judgment or by a notarised document or securityissued by a third party;

6. has been convicted of, and effectively sentenced for, a crime against property or the economy, unless subsequently rehabilitated.

(2) The requirement under paragraph 1, subparagraph 6, shall apply also to the bidder's managers or, as the case may be, members of governance.

(3) The facts and circumstances under paragraph 1 shall be certified by theappropriate competent authority.

Article 102

(1) No bidder shall be deemed to be reliable for the purposes of security if:

1. such bidder is found, on the basis of data, not to meet the requirementsunder Article 41;

2. any of the persons nominated by the bidder for background investigation are found not to meet the security requirements under Article 40.

(2) In the circumstances under paragraph 1, subparagraph 2, the bidder may nominate substitute persons.

(3) The bidder's background investigation for the purposes of paragraph 1 shall be conducted by the security services.

Article 103

(1) Based on the result of the background investigation, the investigating authority shall either issue or deny security certificate.

(2) Security certificate shall be denied where the bidder does not meet therequirements under Article 100.

(3) The denial under paragraph 2 shall not be accompanied with an explanation of reasons and shall only set out the legal reasons for denial.

Article 104

(1) Security certificates and denials to issue such certificates shall be issued on such sample form as SISC shall approve, and shall set out:

1. The competent authority.

2. The name, the registered office, and the BULSTAT Number of the bidder who is issued or denied

certificate.

3. The legal reasons for issuance or denial.

4. The number of the certificate or denial.

5. The certificate's term of validity.

6. The date and place of issuance or denial.

7. The signature and stamp of the issuing authority.

(2) The certificate, and the denial thereof, are written documents and shall be issued in triplicate, to be kept, one each, by SISC, the investigating authority, and the bidder.

Article 105

The head of the organisational unit which is the principal under the contract shall designate a person to exercise control of compliance with the provisions of this Act and the implementing statutory instruments hereto, and to consult the contractor during contract performance.

Article 106

The certificate shall be issued with a term of validity of three years or equal to the duration of the contract, whichever period is shorter.

Article 107

If necessary, a new background investigation shall be conducted at the contractor's request filed with the investigating authority not later than three months before the expiration of the existing certificate.

Article 108

(1) The authority which issued the certificate shall exercise control to ensure that the contractor is currently in compliance with the security requirements hereunder.

(2) Where the holder of a security certificate no longer meets the requirements under Article 100(1), the issuing authority shall prescribe atime limit for the removal of irregularities, provided that the these have not already resulted in unauthorised access to classified information.

(3) Where the holder of a security certificate no longer meets any of the requirements under Article 100(2) or (3), and has failed to remove the irregularities within the time limit under paragraph 2, or it has been established that the irregularity under Article 100(1) has resulted in unauthorised access to classified information, the security certificate shall be revoked by the issuing authority.

Article 109

The denial under Article 103(2) and the revocation of security certificate shall not be appealable before the courts of law, but shall be subject to appeal pursuant to Articles 62-68.

Article 110

(1) The data gathered in the course of background investigations pursuant to this Section shall be kept by the appropriate investigation authority ina separate file and shall be protected as classified information.

(2) The data contained in the files under paragraph 1 may be used for the purposes of this Act.

(3) The files under paragraph 1 shall be kept for a period of 20 years commencing with the date of termination of the contractor's activities.

(4) The special rules for the opening, the storing, the maintenance, the updating, the card-filing, and the

closing of background investigation files shall be laid down in the Detailed Rules for the Application hereof.

Article 111

The protection of classified information in the field of inventions and utility models shall be ensured in accordance with the provisions of the Patents Act, except as otherwise may be provided hereunder.

Article 112

The persons under Article 95(1), having been issued with security certificate in pursuance of this Section, shall have all the duties of organisational units hereunder.

Chapter Seven

DISCLOSURE OR EXCHANGE OF CLASSIFIED INFORMATION

BY THE REPUBLIC OF BULGARIA TO, OR WITH, ANOTHER

STATE OR AN INTERNATIONAL ORGANISATION

Article 113

(1) The Republic of Bulgaria discloses or exchanges classified information to, or with, States or international organisations where international treaties on the protection of such information exist between the Republic of Bulgaria and such States or international organisations.

(2) Where an international treaty under paragraph 1 does not provide for the applicable law with regard to any matters not provided for thereunder, the applicable law shall be that of the party of information source.

Article 114

The decision to disclose or exchange information in pursuance of Article 113(1) shall be made by SISC on the basis of the preliminary opinion of theorganisational unit which releases such information.

Article 115

(1) In accordance with the relevant international treaty, SISC and the competent information security authority of the other State or of the international organisation must, on a reciprocal basis and prior to the disclosure or exchange of information, ensure that such information will beproperly protected.

(2) For the purposes of paragraph 1, the competent information security authority of the other State or of the international organisation must certify before SISC that the persons who will have access to the information disclosed or exchanged are duly cleared for access to information classified at the appropriate or at a higher level.

Article 116

With respect to classified information exchanged with, or disclosed to, theRepublic of Bulgaria by an international organisation of which the Republicof Bulgaria is a member, such protection of classified information principles, norms, and procedures shall apply, as exist within such international organisation, if such an obligation derives from the Republicof Bulgaria's membership of such organisation.

Chapter Eight

ADMINISTRATIVE PENALTIES

Article 117

(1) Whoever commits an offence under Article 17 shall be liable to a fine from BGN 2,000 to 20,000.

(2) Where an offence under Article 17 has been committed by a legal person,such person shall be liable to pay damages from BGN 2,000 to 20,000.

(3) For failure to prevent an offence under paragraph 2, a legal person's chief executive shall be liable to a fine from BGN 1,000 to 5,000, unless the offence is a criminal one.

Article 118

(1) Whoever commits an offence under Articles 18 and 19 shall be liable to a fine from BGN 50 to 300.

(2) The fine under paragraph 1 shall be imposed also on any head of organisational unit or any information security officer who fails to prevent an offence under Articles 18 and 19.

Article 119

Any information security officer who commits an offence under Article 22 shall be liable to a fine from BGN 100 to 1,000.

Article 120

(1) Whoever commits an offence under Article 31 shall be liable to a fine from BGN 100 to 500.

(2) The fine under paragraph 1 shall be imposed also on any head of organisational unit or any information security officer who fails to prevent an offence under Article 31.

Article 121

Any person under Article 31(1) who commits an offence under Article 35(4) shall be liable to a fine from BGN 100 to 1,000.

Article 122

(1) Any official person who commits an offence under Article 43(6) shall beliable to a fine from BGN 50 to 5,000, unless the offence is a criminal one.

(2) The fine under paragraph 1 shall be imposed also on any head of organisational unit or any information security officer who fails to prevent an offence under Article 43(6).

Article 123

Any head of organisational unit or information security officer who commitsor fails to prevent an offence under Article 73(1) shall be liable to a fine from BGN 50 to 400.

Article 124

(1) Whoever commits an offence under Article 86 shall be liable to a fine from BGN 2,000 to 10,000.

(2) Where an offence under Article 86 has been committed by a legal person in the course of its operations, such person shall be liable to pay damagesfrom BGN 3,000 to 15,000.

(3) For failure to prevent an offence under paragraph 1, a legal person's chief executive shall be liable to a fine from BGN 300 to 2,000.

Article 125

Any head of organisational unit who commits or fails to prevent an offence under Article 90(2), second sentence, shall be liable to a fine from BGN 300 to 2,000.

Article 126

Any head of organisational unit who commits or fails to prevent an offence under Article 92 shall be

liable to a fine from BGN 500 to 1,000.

Article 127

(1) Whoever commits or fails to prevent an offence under Article 93 shall be liable to a fine from BGN 500 to 1,000.

(2) Any head of organisational unit who fails to prevent an offence under Article 93 shall be liable to a fine from BGN 1,000 to 2,000.

Article 128

(1) Whoever commits an offence under Article 96 shall be liable to a fine from BGN 1,000 to 3,000.

(2) Any legal person who commits an offence under paragraph 1 shall be liable to pay damages from BGN 1,000 to 5,000.

(3) Any head of organisational unit or information security officer who commits or fails to prevent an offence under Article 96 shall be liable to the fine from BGN 500 to 1,000, unless the offence is a criminal one.

Article 129

(1) Whoever commits or fails to prevent an offence under Article 98(2) shall be liable to a fine from BGN 500 to 1,000.

(2) Where an offence under paragraph 1 has been committed by a legal personin the course of its operations, such person shall be liable to pay damagesfrom BGN 1,000 to 5,000.

Article 130

(1) Whoever commits or fails to prevent an offence under Article 108(3) shall be liable to a fine from BGN 500 to 2,000, unless the offence is a criminal one.

(2) Where an offence under paragraph 1 has been committed by a legal personin the course of its operations, such person shall be liable to pay damagesfrom BGN 1,000 to 3,000.

Article 131

Any head of organisational unit who fails to disclose information to the competent authorities as requested under the conditions and procedure of this Act shall be liable to a fine of BGN 500.

Article 132

Where no other penalty is provided for an offence under this Act and the implementing statutory instruments hereto, the offender shall be liable to a fine from BGN 30 to 200.

Article 133

Where an offence under Articles 117-132 is a repeated offence, the fine, oras the case may be, the damages imposed shall be equal to double the original amounts.

Article 134

(1) The statement establishing an offence under any of the foregoing Articles shall be drawn up by such official persons as the chairperson of SISC, or the head of the National Security Service of the Ministry of Home Affairs, or of the Military Police and Military Counterintelligence Security Service of the Minister of Defence, or of the Communication Devices Protection Directorate of the Ministry of Home Affairs, shall authorise, and the relevant penal order shall be issued by the chairperson of SISC or, within his respective terms of reference, by the appropriate head of service.

(2) The offences hereunder shall be established, and the relevant penal orders shall be issued, appealed, and enforced, under the procedure laid down in the Administrative Offences and Penalties Act.

OTHER PROVISIONS

§ 1. Within the meaning of this Act:

1. "security services" are the National Intelligence Service, the National Security Service, the National Security Service of the Ministry of Home Affairs, the Communication Devices Protection Directorate of the Ministry of Home Affairs, the Operational Searches Directorate of the Ministry of Home Affairs, the Technical Operational Information Directorate of the Ministry of Home Affairs, the Military Information Service of the Ministry of Defence, and the Military Police and Military Counterintelligence Security Service of the Ministry of Defence;

2. "public order services" are the National Police Service of the Ministry of Home Affairs, the National Service for Combating Organised Crime of the Ministry of Home Affairs, the National Border Police Service of the Ministry of Home Affairs, the National Gendarmerie Service of the Ministry of Home Affairs, and the National Fire and Accident Safety Service of the Ministry of Home Affairs;

3. "organisational unit" are: any government authority and its administration, including its divisions, subdivisions, and structural units, and the Armed Forces of the Republic of Bulgaria, and any authority of local self-government and local administration, and any public-law entity created by law or by an instrument of the executive branch, and any natural or legal person which generates, processes, stores or releases classified information;

4. "information security officer" is any natural person, such as appointed by the head of an organisational unit to perform the activities relating tothe protection of classified information within such organisational unit;

5. "competent authority", for the purposes of issuance, termination, revocation, and denial of clearance for access to classified information, is SISC, the head of any security service or public order service, and any information security officer;

6. "unauthorised access to classified information" is the divulgence, misuse, modification, damage, disclosure, destruction of classified information, and any other action compromising the protection, or resultingin the loss of such information. Unauthorised access shall be deemed to be also any omission to classify information by the appropriate marking, or the improper choice of classification marking, and any action or omission resulting in knowledge of such information being acquired by any person whodoes not possess the appropriate clearance or confirmation;

7. "registry" is a separate structure which registers, receives, sends, distributes, prepares, reproduces, releases, and stores classified information;

8. "registry in the field of international relations" is a registry createdin pursuance of an international treaty to which the Republic of Bulgaria is a party;

9. "security marking" is the marking on any material containing classified information which shows the classification level of such material;

10. "material" is any document or any other object of technical nature, or facility or equipment or device or armament, whether finished or in process, and any component thereof used in the manufacture thereof;

11. "document" is any recorded information, regardless of the physical formor characteristics thereof, including the following information media: any handwritten or typed material, any data processing software, any stamp, map, table, photograph, drawing, colouring, etching, technical drawing, or any

part thereof, and any sketch, draft copy, preparatory notes, carbon copy, ink ribbon, and any form of reproduction by any device or process, such as sound, voice, magnetic recording, video recording, electronic recording, optical recording, and any portable equipment or device for electronic data processing on fixed or removable media, etc;

12. "compilation of materials and/or documents" is any number of materials and/or documents brought together for any purpose under this Act, and relating to a single subject and arranged in certain order;

13. "national security" is such a state of society and government which ensures the protection of the fundamental human and civil rights and freedoms, the territorial integrity, the independence and the sovereignty of the country, and the democratic functioning of the State and civil institutions, as a result of which the nation is capable of sustaining and augmenting its prosperity, and of developing;

14. "interests of the Republic of Bulgaria as relate to national security" is the safeguarding of the sovereignty, the territorial integrity, and the constitutional order of the Republic of Bulgaria, including: (a) the detection, prevention, and counteraction of any action detrimental to the country's independence and territorial integrity; (b) the detection, prevention, and counteraction of any covert action posing a threat or causing a prejudice to the country's political, economic, and defence interests; (c) the procurement of information about other countries or of foreign origin, such as is necessary for decisions to be made by the supreme authorities of the State and organs of governance; (d) the detection, prevention, and counteraction of any covert action aimed at a violent change of the country's constitutional order, which guarantees the exercise of human and civil rights, and democratic representation on the basis of a multi-party system, and the functioning of the institutions established by the Constitution; (e) the detection, prevention, and counteraction of any terrorist action, or the illegal trafficking in human beings, weapons, and drugs, and the illegal trafficking in products and technologies placed under international control, and money laundering, or any other specific risks and threats;

15. "damage in the field of national Security, defence, foreign policy or the protection of the constitutional order" is any threat or prejudice to the interests of the Republic of Bulgaria, or to such interests as the Republic of Bulgaria has undertaken to safeguard, the harmful consequences of which are incapable of being eliminated or are only capable of being mitigated by subsequent measures. Depending on the importance of such interests, and on the gravity of such harmful consequences, the damage threatened or caused can be irreparable or exceptionally grave or nearly irreparable or grave or limited, where: (a) irreparable or exceptionally grave damage is such as entails or might entail the complete or partial disruption of the national security or of the related interests of the Republic of Bulgaria as fundamental protected interests; (b) nearly irreparable or grave damage is such as entails or might entail a significant negative impact on the national security or on the related interests of the Republic of Bulgaria as fundamental protected interests, which is incapable of being compensated without harmful consequences or without such harmful consequences as are only capable of being mitigated byconsiderable subsequent measures; (c) limited damage is such as entails or might entail a negative impact of short duration on the national security or the related interests of the Republic of Bulgaria as fundamental protected interests, which is capable of being compensated without harmful consequences or with such harmful consequences as are capable of being mitigated by minor subsequent measures;

16. "repeated" is such an offence under this Act or the implementing statutory instruments hereto as is committed within one year from the effective date of the penal order whereby a penalty was imposed for the same kind of offence;

17. "systematic offences" are three or more offences under this Act or the implementing statutory instruments hereto committed within any one year;

18. "generation, processing, storing, or release of classified information"is the generation, the marking, the registration, the storing, the use, thedisclosure, the transformation, and the declassification of classified information.

§ 2. Within the meaning of this Act, "official person" is any person under Article 93(1) of the Criminal Code.

TRANSITIONAL AND FINAL PROVISIONS

§ 3. Within three months from the entry into force of this Act, the Council of Ministers shall adopt the Detailed Rules for the Application hereof.

§ 4. Within three months from the entry into force of this Act, the Council of Ministers shall:

1. adopt the regulations under Articles 13, 78, 85, 90(1), and 95(2);

2. bring into consistency with this Act the Secret Patents Regulation (SG No. 81/1993), subject to the advice of the chairperson ofthe Patents Office.

§ 5. Within three months from the entry into force of this Act, the Ministerof Health shall, in consultation with SISC, issue the regulation under Article 42(3).

§ 6. Within one month from the entry into force of this Act, the Council of Ministers shall create the State Information Security Commission and shall adopt its Institutional Rules.

§ 7. Within three months from the entry into force of this Act, the heads organisational units shall appoint information security officers, exceptingthe circumstances under Article 20(3), and shall create administrative security units in pursuance of Article 23.

§ 8. Within three months from the entry into force of this Act, the heads oforganisational units and the heads of the security services and the public order services shall draw up the lists under Article 37.

§ 9. (1) Any materials and documents prepared before the entry into force ofthis Act, and marked as "Top Secret of Special Importance", "Top Secret", or "Secret", shall be deemed to be marked respectively as "Top Secret", "Secret", and "Confidential", and the respective durations of classification shall be determined in pursuance of Article 34(1) and shall be deemed to have commenced with the date of preparation such material or document.

(2) Within one year from the entry into force of this Act, the heads of organisational units shall review and bring into consistency with this Act and the implementing statutory instruments hereto the materials and documents which contain classified information.

§ 10. (1) The access permits issued in pursuance of the provisions existing before the entry into force of this Act shall continue to be valid until the replacement thereof with clearances for access. The heads of organisational units, employing persons who possess an access permit and whose positions or special assignments require access the classified information, shall request the issuance of clearances for access in accordance with the requirements of this Act and within three months from its entry into force. Non-compliance with this provision shall result in the invalidation of the existing access permits.

(2) The background investigation and clearance procedure for the purposes of paragraph 1 shall be completed within such time limit as SISC shall prescribe, but not exceeding 18 months.

§ 11. (Corrected, SG No. 5/2003) Any pending issuance procedure for an access permit to secret information shall be transformed into a background investigation procedure under this Act.

§ 12. In Article 20(1), subparagraph 2, of the Cadastral Survey and Property Register Act (SG No. 32/2000), the words "protect asan official secret the data which came to his knowledge" are replaced with the words "protect the classified information, being an official secret, which came to his knowledge".

§ 13. Article 20 of the Constitutional Court Act (SG No. 67/1991, amended, SG No. 25/2001) is amended as follows;

1. In paragraph 2, the words "State or official secret" are replaced with the words "classified information which is a State secret or an official secret".

2. New paragraph 3 is inserted as follows:

"(3) In the circumstances under paragraph 2, the conditions and procedure laid down in the Protection of Classified Information Act shall apply."

§ 14. The Republic of Bulgaria Defence and Armed Forces Act (SG No. 112/1995, amended and supplemented SG 67/1996, SG 122/1997, SG 70, 93, 152 and 153/1998, SG. 12, 67 and 69/1999, SG 49 and 64/2000, SG 25/2001, SG 1 and 40/2002 amended) is amended as follows:

1. In Article 5, the words "State or official secret" are replaced with thewords"classified information which is the State or an official secret".

2. Article 32(9) is repealed.

3. In Article 35(1), subparagraph 14, the words "State or official secret"are replaced with the words "classified information which is a State secretor an official secret".

4. In Article 78(1), subparagraph 16, the words "State or official secret"are replaced with the words "classified information which is the State or an official secret".

5. In Article 200, the words "State or official secret" are replaced with the words "classified information".

6. In Article 273, the words "State or official secret" are replaced with the words "classified information".

7. In Article 281(1), the words "State or official secret" are replaced with the words "classified information which is the State or an official secret".

§ 15. In Article 9(2) of the Foreign Exchange Act (SG No. 83/1999), the words "and official secret" are replaced with the words "secret and the requirements relating to the protection of classified information which is an official secret".

§ 16. In Article 3 (3) of the Carriage by Road Act (SG No. 82/1999, amended, SG No. 11/2002), the word "official" are replaced with the words "classified information which is an official secret".

§ 17. In Article 15 (3) of the Administrative Procedure Act (SG No. 90/1979, amended, SG No. 9/1983, 26/1988, 94/1990, 25 and 61/1991, 19/1992, 65 and 70/1995, 122/1997, 15 and 89/1998, 83 and 95/1999), the words "protection of" are replaced with the words "protection of classified information which is".

§ 18. In § 5 of the Other Provisions of the Refugees Act (SG No. 53/1999, amended), the words "official secret" are replaced with the words "classified information which is an official secret".

§ 19. In Article 52 of the Banks Act (SG No. 52/1997, amended and supplemented, SG No. 15, 21, 52, 70 and 89/1998, 54, 103 and 114/1999, 24, 63, 84 and 92/2000, 1/2001), new paragraph 8 is inserted as follows:

"(8) The banks shall have a duty, at the written request of the chairpersonof SISC or of the head of any security service or public order service, to provide information about the account balances and transactions of any person under a background investigation pursuant to the Protection of Classified Information Act. Such request shall be accompanied by such person's consent to the disclosure of such information."

§ 20. The Bulgarian Personal Identity Documents Act (SG No. 93/1998, amended, SG No. 53, 67, 70 and 113/1999, 108/2000, 42/2001) is amended as follows:

1. In Article 75, new paragraph 2 is inserted as follows:

"2. persons about whom sufficient evidence exists that by such travel they might pose a threat to the system for the protection of classified information which is the State secret of the Republic of Bulgaria;"

2. In Article 78, the existing text is placed under paragraph 1 and new paragraph 2 is inserted as follows:

"(2) The involuntary administrative measure under Article 75(2) shall be taken in pursuance of a reasoned order of the chairperson of the State Information Security Commission or of the head of any security service or public order service."

3. In Article 79(1) and (2), the reference "Article 75(1) and (3)" are replaced with the reference "Article 75 (1) - (3)".

§ 21. The Ministry of the Interior Act (SG No. 122/1997, Judgment No. 3/1998 of the Constitutional Court - SG No. 29/1998, amended, SG No. 70, 73 and 153/1998, 30 and 110/1999, 1 and 29/2000, 28/2001) is amended as follows:

1. In Article 7(14), the words "encryption operations within the Republic of Bulgaria and within its representations abroad" are replaced with the words "cryptographic protection of classified information within the Republic of Bulgaria and within its diplomatic and consular missions".

2. In Article 46(1), subparagraph 7, the words "protection of the facts, information, and objects which are a State secret" are replaced with the words "protection of classified information which is a State secret or an official secret".

3. Article 51(1) is amended as follows:

"(1) The National Security Service performs activities in connection with the functioning of the National System for the Protection of Classified Information which is a State Secret or an Official Secret in pursuance of the Protection of Classified Information Act."

4. In Article 52(1), the words "protection of the facts, information, and objects which are a State secret" are replaced with the words "protection of classified information".

5. Article 53 is repealed.

6. Article 124 is amended as follows:

"124. (1) The Communication Devices Protection Directorate is a special directorate of the Ministry of Home Affairs responsible for the cryptographic protection of classified information within the Republic of Bulgaria and within its diplomatic and consular missions, and for the acquisition, organisation and processing of information from foreign sources in the interest of national security, and for the operational control of the national radio frequency spectrum, by:

1. evaluation and development of cryptographic algorithms and devices for cryptographic protection of classified information; development and distribution of cryptographic keys; approval and control of the use, manufacture and import of cryptographic protection devices;

2. issuance of security certificates of automated information systems or networks used for classified information; coordination and control of the electromagnetic interference countermeasures protecting the technical devices used for the processing, the storing, or the transmission of classified information;

3. organisation and operation of the communications between the Republic ofBulgaria and its diplomatic and consular missions, and cryptographic protection of the information so exchanged by the provision of the necessary personnel for the departmental units and for the diplomatic and consular missions;

4. acquisition, processing, and organisation of information by technical devices from the technical sources of other States in the interest of national security, and release of such information to such users as shall be designated by an order of the Minister of Home Affairs or by law;

5. detection and prevention of any use of the national radio frequency spectrum against the country's security or contrary to the law, and joint actions with the competent government authorities;

6. provision and use of special surveillance devices, and preparation of investigation exhibits under such conditions and procedure has shall be provided by law;

7. operational searches;

8. joint actions with the other services of the Ministry of Home Affairs and with the special government authorities, and with the counterpart services of other States, within its terms of reference;

9. information activities.

(2) The relevant departments shall provide funding support to the units under paragraph 1, subparagraph 3, and such units within diplomatic or consular missions.

(3) The organisation of activities under paragraph 1, subparagraph 3, shallbe provided for by a regulation of the Council of Ministers."

7. Article 162(3) is repealed.

8. In Article 187, the words "protection of the facts, information, and objects which are a State secret" are replaced with the words "protection of classified information".

§ 22. The Bulgarian National Bank Act (SG No. 46/1997, amended, SG No. 49 and 153/1998, 20 and 54/1999, 109/2001) is amended as follows:

1. In Article 4(2), after the words "credit relations", a comma is inserted and the words "excepting the circumstances under the Protection ofClassified Information Act".

2. In Article 23(2), the words "which are an official" are replaced with the words "which is classified information, being an official".

§ 23. The Access to Public Information Act (SG No. 55/2000, amended SG No. 1/2002) is amended as follows:

1. In Article 7(1), the word "is" is replaced with the words "is classified information, being".

2. In Article 9(2), the words "State or official secret" are replaced withthe words "classified information which is a State or an official secret".

3. In Article 13(3), the words "20 years" are replaced with the words "twoyears".

4. In Article 37(1), subparagraph 1, the words "State or official secret" are replaced with the words "classified information which is a State or an official secret".

5. In Article 41(4), the word "classification" is replaced with the words "placement of security marking".

§ 24. The State Property Act (SG No. 44/1996, amended, SG No. 104/1996, 55, 61 and 117/1997, 93 and 124/1998, 67/1999, 9, 12, 26 and 57/2000, 1/2001; Judgment No. 7/2001 of the Constitutional Court - SG No. 38/2001) is amended as follows:

1. In Article 70(2), the words "State secret" are replaced with the words "classified information which is a State or an official secret".

2. In Article 78(2), the words "State secret" are replaced with the words "classified information which

is a State or an official secret".

§ 25. Article 25 of the Civil Servants Act (SG No. 67/1999, amended SG No. 1/2000, 25, 99 and 110/2001) is amended as follows:

"Protection of Classified Information Which Is a State or an Official Secret

25. (1) Every civil servant shall have a duty to protect the classified information, which is a State or an official secret, which came to his knowledge in the course of, or in connection with, the pursuance of his official duties.

(2) The classified information which is a State or an official secret, and procedure for operation therewith, shall be defined by law."

§ 26. Article 17 of the Act Restoring Ownership of Forests and Forest Stock Land Tracts (SG No. 110/1997, amended, SG No. 33, 59 and 133/1998, 49/1999, 26 and 36/2001) is amended as follows:

1. The existing text is placed under paragraph 1 and the words "including such as are a State secret" are deleted.

2. New paragraph 2 is inserted as follows:

"(2) Where the information under paragraph 1 is classified information, therelease thereof shall be governed by the Protection of Classified Information Act."

§ 27. In Article 11(1) of the Postal Services Act (SG No. 64/2000, amended SG No. 112/2001), the words "secret correspondence" are replaced with the words "correspondence which contains classified information".

§ 28. Article 9 of Decree No. 612, Chapter 2, on Seals and Stamps (SG No. 69/1965, amended, SG No. 26/1988, 11 and 47/1998) is repealed.

§ 29. In Article 6 (1) of the Public Procurement Act (SG No. 56/1999, amended, SG No. 92 and 97/2000, 43/2002), the words "are the subject of a State secret" are replaced with the words "are the subject of classified information which is a State secret".

§ 30. The Statistics Act (SG No. 57/1999, amended, SG No. 42/2001) is amended as follows:

1. In Article 22, the words "protection of secrets" are replaced with the words "protection of classified information".

2. Article 27(2) is amended as follows:

"(2) The registration, the use, the processing, and the storing of statistical data which are classified information shall be governed by the provisions of the legislative and the statutory instruments relating to theprotection of classified information."

§ 31. The Audit Office Act (SG No. 109/2001) is amended as follows:

1. In Article 30(1), the words "State, official" are replaced with the words "classified information which is a State or an official secret, and".

2. In Article 31, new paragraph 7 is inserted as follows:

"(7) Where the exercise of the powers under paragraph 1 requires access to classified information, the relevant conditions and procedure laid down in the Protection of Classified Information Act shall apply."

§ 32. Article 6 (2), second sentence, of the Act to Transform the Construction Corps, the Transport Ministry Troops and the Posts and Telecommunications Committee Troops into State-Owned Enterprises (SG No. 57/2000) is amended as follows:

"They can perform and award public procurement contracts relating to the country's defence or security and having as their subject matter classifiedinformation which is a State secret, and the performance thereof shall be governed by the provisions of the Protection of Classified Information Act."

§ 33. Article 32(2) of the Social Assistance Act (SG No. 56/1998) is amended as follows:

"(2) The inspectors shall have a duty to comply with the provisions of the legislative and the statutory instruments relating to the protection of classified information with regard to such information as came to their knowledge in the course of, or in connection with, an inspection, and shallhave a duty to respect the honour and the dignity of the assistance beneficiaries."

§ 34. The Patents Act (SG No. 27/1993, amended, SG No. 11/1998, 81/1999) is amended as follows:

1. Article 24 is amended as follows:

"24. (1) Secret patents shall be issued with respect to inventions which contain classified information which is a State secret within the meaning of Article 25 of the Protection of Classified Information Act.

(2) At the filing of a secret patent statement, the applicant shall have a duty to state that the subject invention is a matter of State secret.

(3) The level at which the invention under paragraph 2 shall be classified shall be determined by the appropriate competent authority, to the activities of which the invention relates, subject to consultation with theState Information Security Commission.

(4) The competent authority under paragraph 3 shall decide within three months from the date of referral and shall advise the Patents Office accordingly. The secret patent statement shall be identified with the appropriate security marking, in accordance with the competent authority's decision, and the applicant shall be advised accordingly.

(5) If, within the time limit under paragraph 4, the Patents Office is not advised of classification level, the subject statement shall be deemed to be free of any information which is a State secret. The Patents Office shall advise the applicant that the subject invention does not contain any classified information which is a State secret and shall require the applicant's express consent to the review of his statement under the general procedure. If the applicant fails to give such consent, the statement shall be deemed to have been withdrawn and the relevant materialsshall be returned to the applicant.

(6) Where the competent authority under paragraph 3 is an applicant and where, subject to consultation with the State Information Security Commission, the statement has been security-marked in accordance with the classification level of the invention, the procedure under paragraphs 4 and5 shall not apply.

(7) The Patents Office shall only publish the numbers of secret patents issued, at no charge."

2. Article 25(2) is amended as follows:

"(2) The competent authorities under Article 24(3) may, subject to consultation with the State Information Security Commission, ban the patenting abroad of any invention which contains classified information which is a State secret."

3. In Article 31(5), the words "subject to the prior written consent of the Ministry of Defence or the Ministry of Home Affairs" are replaced with the words "under the conditions and procedure laid down in the Protection of Classified Information Act".

4. In Article 32(8), the words "only by the Council of Ministers, at the request of the Ministry of Defence or of the Ministry of Home Affairs" are replaced with the words "by the State Information Security Commission".

5. In Article 45(3), the words "the Ministry of Defence or of the Ministryof Home Affairs" are replaced

with the words "the competent authorities under Article 24(3), subject to consultation with the State Information Security Commission".

6. Article 46(3) is repealed.

7. In Article 48, the reference "Article 46(1), (2), and (3)" is replaced with the reference "Article 46(1) and (2)".

8. Article 50 is amended as follows:

(a) paragraph 1, subparagraph 3, is amended as follows:

"3. the statement is made for the issuance of a secret patent for an invention which contains classified information which is a State secret;"

(b) paragraph 3 is amended as follows:

"(3) The Patents Office shall publish where, pursuant to Article 34 of the Protection of Classified Information Act, no legal reasons exist any longerfor the classification of information contained in the invention as a Statesecret."

9. In Article 55(1), subparagraph 1, the reference "Article 46(2) and (3)" is replaced with the reference "Article 46(2)".

10. Article 67(6) is amended as follows:

"(6) Where the Republic of Bulgaria designates itself in pursuance of Article 8(2), subparagraph (b), of the Treaty, the Patents Office shall refer the international statement to the competent authorities, to the activities of which such invention relates, for the determination of a classification level. Such determination shall be governed by the provisions laid down in the Protection of Classified Information Act and shall be completed within the time limit under Article 24(4) of the same. If it is established that such international statement contains informationclassified as a State secret, it shall not be treated as an international statement and shall not be distributed officially and shall not be published."

11. In Article 84(1), the words "secret statement" are replaced with the words "secret patent statement", and the words "from BGN 100 to 1,000" are replaced with the words "from BGN 1,000 to 20,000".

§ 35. In Article 99 (1) of the Telecommunications Act (SG No. 93/1998, amended, SG No. 26/1999, 10 and 64/2000, 34, 42, 96 and 112/2001), the words "national encryption authority" are replaced with the words "Communication Devices Protection Directorate".

§ 36. In Article 33 (2) of the Local Self-government and Local Administration Act (SG No. 77/1991, amended, SG No. 24, 49 and 65/1995, 90/1996, 122/1997, 33, 130 and 154/1998, 67 and 69/1999, 26 and 85/2000, 1/2001, 28/2002), the words "State or official secret within the meaning of the law" are replaced with the words "classified information which is a State or an official secret".

§ 37. (1) The Access to the Documents Act of the Former State Security Police and the Former Intelligence Service of the General Staff (SG No. 63/1997, as Judgment No. 10/1997 of the Constitutional Court - SG No. 89/1997, amended, SG No. 69/1999, 24/2001; Judgment No. 14/2001 of the Constitutional Court - SG No. 52/2001; amended, SG No. 28/2002) is repealed.

(2) The appropriations under the National Budget Act for 2002 to, and the fixed tangible assets of, the government authorities under the Access to the Documents Act of the Former State Security Police and the Former Intelligence Service of the General Staff, which have ceased to exist, shall be transferred to the State Information Security Commission.

§ 38. Articles 284a and 313b of the Criminal Code (SG No. 26/1968, corrected, SG No. 29/1968, amended and supplemented, SG No. 92/1969, 26 and 27/1973, 89/1974, 95/1975, 3/1977, 54/1978, 89/1979, 28/1982; corrected, SG No. 31/1982; amended and supplemented, SG No. 44/1984, 41 and

79/1985; corrected, SG No. 80/1985; amended and supplemented, SG No. 89/1986; corrected, SG No. 90/1986; amended, SG No. 37, 91 and 99/1989, 10, 31 and 81/1990, 1, 86, 90 and 105/1991, 54/1992, 10/1993, 50/1995; Judgment No. 19/1995 of the Constitutional Court - SG No. 97/1995; amended, SG No. 102/1995, 107/1996, 62 and 85/1997; Judgment No. 19/1997 of the Constitutional Court - SG No. 120/1997; amended, SG No. 83, 85, 132, 133 and 153/1998, 7, 51 and 81/1999, 21 and 51/2000; Judgment No. 14/2000 of the Constitutional Court - SG No. 98/2000; amended, SG No. 41/2001, 101/2001) are repealed.

§ 39. Article 24 (1), subparagraphs 9 and 10, Article 29 (2), Article 48 (5), and § 6 of the Transitional and Final Provisions, of the Election of National Representatives Act (SG No. 37/2001, Judgment No. 8/2001 of the Constitutional Court - SG No. 44/2001) are repealed.

§ 40. Article 42a of the Election of Grand National Assembly Act (SG No. 28/1990, amended, SG No. 24/2001) is repealed.

§ 41. Article 8 (2) of the Election of President and Vice President of the Republic Act (SG No. 82/1991, amended, SG No. 98/1991, 44/1996, 59/1998, 24, 80 and 90/2001) is repealed.

§ 42. Article 42 (4) of the Local Elections Act (SG No. 66/1995, corrected, SG No. 68/1995; Judgment No. 15/1995 of the Constitutional Court - SG No. 85/1995; amended, SG No. 33/1996; Judgment No. 4/1998 of the Constitutional Court - SG No. 22/1998; amended, SG No. 11 and 59/1998, 69 and 85/1999, 29/2000, 24/2001) is repealed.

§ 43. The List of Facts, Data and Objects Which Are a State Secret of the Republic of Bulgaria (SG No. 31/1990, amended, SG No. 90 and 99/1992, 108/1999, 55/2000) is repealed.