OFFICIAL TRANSLATION

REPUBLIC OF LITHUANIA

LAW ON STATE SECRETS AND OFFICIAL SECRETS

25 November 1999 No VIII-1443

Vilnius

(A new version as of 16 December 2003 No.IX-1908)

CHAPTER I GENERAL PROVISIONS

CHAPTER I GENERAL PROVISIONS

Article 1. Purpose of the Law

Article 1. Purpose of the Law

1. This Law shall regulate the basic principles of and procedure for classifying, storing, using, declassifying of the information comprising a state or official secret, co-ordinating and controlling protection actions and set minimum requirements for separate fields of protection of classified information (personnel security, administration of classified information, physical security, security of classified contracts, protection of automated data processing systems and networks).

2. The classified information of foreign states, the European Union or international organisations released to the Republic of Lithuania shall be stored and used in accordance with the procedure laid down by international treaties of the Republic of Lithuania, decisions of international organisations based on these treaties and implementing them, legal acts of the European Union and this Law. In the cases when international treaties of the Republic of Lithuania and/or decisions of international organisations based on the treaties and/or implementing them and legal acts of the European Union set other requirements for the storage and use of classified information of foreign states or international organisations than specified in this Law, the provisions of the international treaties and/or decisions of international

organisations based on the treaties and/or implementing them and legal acts of the European Union shall apply.

Article 2. Definitions

Article 2. Definitions

1. “Classified information” shall mean the information recognised by an entity of secrets a state or official secret and related to the existence, essence or contents of documents, works, products or other objects as well as the documents, works, products or other objects recognised a state or official secret.

2. “State secret” shall mean the political, military, intelligence, counterintelligence, law enforcement, scientific and technical information classified in accordance with the procedure laid down by this Law, a loss or compromise of which may present a threat to the sovereignty, territorial integrity and defence power of the Republic of Lithuania, cause prejudice to state interests and pose a hazard to the human life. The list of categories of state secrets shall be determined by this Law.

3. “Official secret” shall means the political, military, economic, law enforcement, scientific and technical information classified in accordance with the procedure laid down by this Law, a loss or compromise of which may inflict damage upon interests of the State or institutions thereof or create preconditions for a compromise of the information comprising a state secret and pose a hazard to human health. The list of categories of official secrets shall be determined by this Law.

4. “Classified document” shall mean the recorded information recognised as a state or official secret, regardless of the means of its recording and information-carrying media (graphic works performed by various means: hand-written, published in a printing house, typed, computer-written, painted or drawn; video or audio recordings, computer files, film and photo negatives, positives or other information arrays) as well as copies of such information-carrying media made in any manner or by any means.

5. “Classified products” shall mean a variety of installations, systems, weapons, military, computer and other technical equipment, complexes, aggregates, devices, software and chemical products recognised a state or official secret.

6. “Classified works” shall mean scientific, research, testing, design,

technical maintenance works and technological processes recognised a state or official secret.

7. “Other classified objects” shall mean materials, liquids, gases, minerals, biological and other forms of matter which have been recognised a state or official secret and which, according to their properties or nature, cannot be ascribed to the concept of a document, products or works.

8. “Entities of secrets” shall mean the institutions set up by the President of the Republic, the Seimas and the Government, state and municipal institutions, the undertakings and agencies set up by them, the activities of which are related to the classification and declassification of information, the use of classified information or protection thereof.

9. “Originator of classified information” shall mean an entity of secrets that has prepared and classified information in accordance with the procedure laid down by this Law or the successor to rights thereof.

10. “Recipient of classified information” shall mean an entity of secrets or structural division thereof, a person, contractor (sub-contractor) that has obtained, in accordance with the procedure laid down by legal acts, the classified information prepared by another entity of secrets.

11. “Classification of information” shall mean the assignment of data to a state or official secret, application of an appropriate classification, laying down of a time period for classification and establishing required protection.

12. “Declassification of classified information” shall mean cancellation of a classification applied to data and established protection.

13. “Protection of classified information” shall mean application of protection measures and procedures against a loss or compromise of classified information.

14. “Personnel Security” shall mean the procedures which have been laid down for screening candidacies of the persons applying for authorisations to handle or familiarise with classified information or for security clearances and which allow to decide whether a person may be entrusted with classified information as well as the control and periodic instruction of a person holding an authorisation to handle or familiarise with classified information or a security clearance on requirements for the protection of classified information and statutory liability for violation thereof.

15. “Authorisation to handle or familiarise with classified information”

shall mean a document issued in accordance with the procedure laid down by this Law and confirming a person' s right to handle or familiarise with the Republic of Lithuania information classified "Top Secret ", "Secret", "Confidential" or to store or transport such information.

16. "Security clearance" shall mean a document issued in accordance with the procedure laid down by this Law and confirming a person' s right to handle or familiarise with the classified information released by foreign states or international organisations and classified "Top Secret ", "Secret", "Confidential" or to store or transport such information.

17. "Consent for screening" shall mean a written consent of a person applying for an authorisation to handle or familiarise with classified information or for a security clearance whereby authorised institutions are granted the right to collect and obtain data on him and his contacts as well as the surroundings which influence the assessment of the person' s security and loyalty to the State of Lithuania.

18. "Pledge to protect classified information" shall mean a written commitment of a person holding an authorisation to handle or familiarise with classified information or a security clearance to protect the classified information entrusted or made known to him.

19. "Physical protection" shall mean the totality of the physical, mechanical, electronic and procedural security measures and methods ensuring the protection of the territories and premises in which classified information is handled or is stored against unauthorised access thereto and the protection of the classified information stored therein against seizure, other unauthorised acquisition, compromise and loss. It shall be applied by taking account of classifications of protected information, importance, volume of the information as well as assignment of such territories, premises or workstations to an appropriate security area.

20. "Security area" shall mean an established protected territory or premises intended for handling classified information and protection thereof.

21. "Administration of classified information" shall mean procedures for preparing, formalising, registering, sending, transporting, receiving, reproducing, protecting, destroying and accounting of the classified information which has been assigned different classifications.

22. "Subject to a consent of the originator of information" shall mean a reference denoting that a classified document may not be reproduced or distributed without a consent of the originator of classified information.

23. “Protection of automated data processing systems and networks (hereinafter referred to as “ADP systems and networks”)” shall mean the totality of the mechanical, software, procedural and electronic security measures ensuring the confidentiality of the classified information stored, processed and transmitted in ADP systems and networks, availability to authorised information users and the integrity and authenticity of such information.

24. “Classified contract” shall mean an agreement concluded between an entity of secrets and a legal or natural person on the carrying out, creation, purchase, sale, provision, physical protection, transportation and maintenance of certain works, products or other objects which are themselves or information on which is classified “Top Secret”, “Secret” or “Confidential”.

25. “Security of classified contracts” shall mean the application of classified information security measures and procedures in the course of the conclusion and execution of classified contracts.

26. “Contractor” shall mean a legal or physical person wherewith an entity of secrets is planning to conclude or has concluded a classified contract.

27. “Sub-contractor” shall mean a third party employed by the contractor for the implementation of part of a classified contract.

28. “Facility security clearance” shall mean a document issued in accordance with the procedure laid down by this Law and confirming that a contractor (sub-contractor) has implemented all classified information protection requirements necessary for the execution of a specific classified contract. The requirement to obtain a facility security clearance shall be applied where the contractor (sub-contractor) is a legal person.

29. “Institutions ensuring the security of classified contracts” shall mean the institutions implementing requirements for the security of classified contracts and exercising control prior to signing a classified contract and in the course of execution thereof.

30. “Consent of the contractor (sub-contractor) for inspection” shall mean a written consent of the contractor (sub-contractor) that needs to obtain a facility security clearance whereby the institutions ensuring the security of classified contracts are granted the right to collect and obtain data on the contractor (sub-contractor).

31. “Classification guide” shall mean a document drafted for the execution

of specific classified contracts and specifying the classified information in use or planned to be created, establishing classifications of this information, time periods for classification and conditions of changing of the classifications or declassification of information.

32. “Employee” shall mean a public servant or a person employed under a work contract or a serviceman.

33. “Responsible person” shall mean a separate structural division (divisions) of an entity of secrets designated by a decision of the head of the entity of secrets or a person authorised by him, an employee or an employee appointed by a decision of the head of the contractor (sub-contractor) to organise and implement the administration, protection and control of the classified information held by the entity of secrets or the contractor (sub-contractor).

Article 3. Basic Principles of Organisation of the Protection of Classified Information

Article 3. Basic Principles of Organisation of the Protection of Classified Information

1. Information must be classified and declassified in conformity with the principles of lawfulness, validity and timeliness.

2. Information must be classified where it corresponds to at least one of the categories of information referred to in Article 7 of this Law and where disclosure or loss thereof is likely to pose a threat to interests of the State or institutions thereof, human life or legal interests of society.

3. A classification applied to information and the level of protection established for such information must be commensurate with the importance of classified information and the amount of the prejudice likely to be caused upon a compromise or loss of such information.

4. An entity of secrets that has classified information must ensure that the classified information, upon the cessation of necessity for classification or where the previously established level of protection of information, according to its importance, is not required any longer, is immediately declassified or such information is downgraded and the entities of secrets whereto such information has been released are notified thereof.

5. Classified information must, at all stages of administration thereof, be afforded required protection throughout the time period for classification thereof.

6. Classified information must be entrusted in strict compliance with the need-to-know principle. The need-to-know principle shall mean that classified information may be entrusted only to the persons holding appropriate authorisations to handle or familiarise with classified information and needing, in discharge of their official duties, to familiarise with classified information. A person may be entrusted with classified information of the volume required for the discharge of his duties.

7. In order to safeguard classified information, requirements for all areas of the protection of classified information (personnel security, administration of classified information, physical security, security of classified contracts, protection of ADP systems and networks) must be applied in the aggregate.

8. All breaches of requirements for the protection of classified information which may result or have resulted in a loss or compromise of classified information must be immediately reported to the head of an entity of secrets, and the latter must take appropriate measures to prevent further disclosure or loss of classified information and to minimise the adverse effects as well as immediately notify thereof authorised institutions. The institutions must, in accordance with the established procedure, conduct an enquiry to establish the facts of the breaches of requirements for the protection of classified information and to prosecute the persons liable therefor.

Article 4. Right of Ownership of Classified Information, Release of Classified Information to Foreign States and International Organisations

Article 4. Right of Ownership of Classified Information, Release of Classified Information to Foreign States and International Organisations

1. Classified information, except for the information considered a secret of foreign states or international organisations, shall be the property of the Republic of Lithuania.

2. When acquiring into the ownership of the State the information which, according to its nature and importance, should be classified, but belongs by

the right of ownership to a natural or legal person that is not an entity of secrets, he must be fairly recompensed. A decision on the acquisition of information into the ownership of the State shall be taken by the Government. The Republic of Lithuania Commission for Secrets Protection Co-ordination (hereinafter referred to as the Commission for Secrets Protection Co-ordination) shall, upon the recommendation of entities of secrets, assess the validity of the acquisition of such information and determine a possible recompense to the holder of the information. Where the holder of the information agrees with the proposed recompense, the entity of secrets shall address the Government for a relevant decision thereon to be taken. Where the holder of the information does not agree with the proposed recompense, information shall be taken into the ownership of the State upon a decision of the Government by recompensing the holder of such information at the price established by the Commission for Secrets Protection Co-ordination. The holder of the information may appeal against such a decision of the Government to courts in accordance with the procedure laid down by laws.

3. The information comprising a state secret may be released only to the states or international organisations with which the Republic of Lithuania has signed agreements on the reciprocal protection of classified information. Such information may be released to the states or international organisations with which the Republic of Lithuania has not signed an agreement on the reciprocal protection of classified information by a decision of the Commission for Secrets Protection Co-ordination.

4. The information comprising an official secret may be released to foreign states or international organisations upon a decision of the head of an entity of secrets or a person authorised by him, where this is required for the performance of functions of the entity of secrets.

CHAPTER II MARKING, CLASSIFICATION, DECLASSIFICATION OF CLASSIFIED INFORMATION

CHAPTER II MARKING, CLASSIFICATION, DECLASSIFICATION OF CLASSIFIED INFORMATION

Article 5. Classification and marking of information

Article 5. Classification and marking of information

1. Classified information shall be divided into top secret, secret, confidential and restricted information according to its importance, the amount of the prejudice likely to be caused to the State, institutions thereof or individuals upon a loss or disclosure of this information to unauthorised persons and the level of protection required to protect such information.

2. Classification "Top Secret" shall be applied to the information comprising a state secret, a loss or compromise of which may pose a threat to the sovereignty or territorial integrity of the Republic of Lithuania or cause exceptionally grave prejudice to state interests or pose a hazard to human life.

3. Classification "Secret" shall be applied to the information comprising a state secret, a loss or compromise of which may impair the defence capabilities of the State or cause prejudice to state interests.

4. Classification "Confidential" shall be applied to the information comprising an official secret, a loss or compromise of which may harm state interests or cause prejudice to activities of state institutions or create preconditions for a compromise of the information comprising a state secret.

5. Classification "Restricted" shall be applied to the information comprising an official secret, a loss or compromise of which may harm interests of state institutions.

6. Classifications, in decreasing order of importance, shall be the following:

1) "Top Secret";

2) "Secret";

3) "Confidential";

4) "Restricted".

7. The application of the classifications of information as specified in this Article to the information not specified by this Law shall be prohibited.

Article 6. Classification of Information

Article 6. Classification of Information

1. Information shall be classified on the basis of the list of categories of information to be classified presented in Article 7 of this Law, detailed lists of information to be classified which have been drawn up by entities of secrets on the basis of the list and approved in accordance with the established procedure as well as the contents of specific information to be classified.

2. Classifications of information shall be applied or changed and the time periods for classification thereof shall be established by the entities of secrets which prepared the information in accordance with the procedure laid down by this Law.

3. The head of an entity of secrets' structural division which has prepared and classified information in accordance with the established procedure shall be responsible for the classification of the information and application of valid classifications.

Article 7. List of Categories of Information to be Classified

Article 7. List of Categories of Information to be Classified

1. A state secret may comprise:

1) detailed data on the state military reserve and consolidated detailed data on the mobilisation reserve of material resources;

2) plans of activities of state and municipal institutions under the conditions of a state of emergency and war and mobilisation plans;

3) detailed data on the creation, use, production technologies, technical data of the technological protection means used for the protection of securities, documents, document forms, tax stamps, official markings, banknotes and coins against forgery;

4) detailed information on the use of technological processes for quality upgrading of armaments, military equipment and the technical means used in operational investigative activities;

5) detailed information on negotiations with foreign states or international organisations; the information related to the foreign states or international organisations, a loss or compromise of which may harm relations between the

states, state interests or conclusion of treaties;

6) detailed information on the course, objects, contents and results of co-operation with the special services of foreign states or international organisations;

7) detailed data on organisation of the protection of the State Enterprise Ignalina Nuclear Power Plant;

8) detailed data on cable lines of the networks intended for the transmission of classified information, on systems of launching installations, electricity supply and non-cryptographic protection as well as detailed schemes thereof;

9) data on combination settings, enciphering equipment intended for the enciphering of classified information or protection thereof and on related documents, organisation and carrying out of enciphering operations;

10) data on the equipment and functioning of the information systems processing classified information, the protection means applied thereto;

11) detailed data on the use of radio frequencies and call signs in the event of a war or state of emergency as well as the structure of telecommunications networks, communication schemes and the use of interconnectors and telecommunications networks for the purposes of state security and defence;

12) plans of state defence, control and command of the army and other armed forces;

13) detailed data on the air space surveillance and control system used for state defence;

14) mobilisation plans of the deployment of the army and types thereof and other armed forces, a scheme for managing mobilisation notification and mobilisation deployment as well as information on actions of the army and other armed forces and on control of military units in the event of introduction of alert stages;

15) consolidated detailed data of a register handled by the Weaponry Fund of the Republic of Lithuania under the Government of the Republic of Lithuania (hereinafter referred to as the Weaponry Fund), where the owner, manager, user of a weapon is an institution of the national defence system, institution of the system of the Interior or the system of the State Security Department or entities of operational investigative activities;

16) the information likely to disclose the identity of covert participants in operational investigative activities;

17) detailed data on the record file data of covert participants in operational investigative activities who are insured with state social insurance and compulsory health insurance, on state social insurance and compulsory health insurance contributions, income tax contributions and on the data of property and income declarations of these persons and their family members;

18) detailed data on the organisation, course and results of the operational investigative activities carried out by the structural divisions of the State Security Department as well as the Second Investigation Department under the Ministry of National Defence which are engaged in intelligence or counter-intelligence, the use of measures and methods, financing thereof, provision with technical means of operational investigative activities, other logistical support, the information obtained in the course of operational investigative activities as well as analytical information making use of the information obtained in the course of operational investigative activities;

19) detailed data on the organisation, course and results of the operational investigative activities carried out by entities of operational investigative activities and covert participants in operational investigative activities, the use of measures and methods, financing thereof, logistical support, the information obtained by covert participants in operational investigative activities in the course of the operational investigative actions and the analytical information prepared on the basis thereof;

20) the information which has been voluntarily submitted by present or former employees of or the persons engaged in covert co-operation with of the special services of other states to entities of operational investigative activities;

21) the classified data of a pre-trial investigation or criminal case assisting in the identification of a witness or a victim;

22) the data likely to disclose the identity of the persons who have been granted statutory protection against criminal pressure as well as information on the income tax contributions of these persons, detailed information on the organisation of protection of the said persons and financing thereof;

23) plans of operations to fight terrorism and sabotage;

24) the information related to covert intelligence staff members and the persons engaged in covert co-operation with intelligence services and the special guarantees applied thereto;

25) the information related to the legal persons ensuring operational investigative activities and providing favourable conditions therefor;

26) the analytical information prepared by institutions of national security and related to the assessment of external risks and threats;

27) data on the course of operations and composition of special mission military units of the national defence system;

28) detailed data on new technologies, scientific research, tests and results thereof which are of particular importance for state interests.

2. An official secret may comprise:

1) detailed data on the organisation of protection of classified information, accounting and managing of such information;

2) detailed data on the procedure for and course of screening candidacies of the persons applying for an authorisation to handle or familiarise with classified information as well as the detailed data collected thereon in the course of the screening, where such data are not assigned to a state secret;

3) detailed plans of pre-trial investigation institutions on search for and detention of the persons who have committed, are suspected of or are charged with criminal acts as well as on the organisation of complex means and operations;

4) detailed data on the orgranisation of protection of protected persons of state institutions or structural divisions thereof and important state and military objects, the protection systems in use, documents of design, construction and repairs of such objects;

5) information on the co-operation of entities of operational investigative activities with municipal institutions, undertakings, agencies and organisations for the purposes of operational investigative activities;

6) consolidated detailed data on the logistical support, quantitative and composition of special mission units of the Lithuanian army and entities of operational investigative activities;

7) consolidated detailed data on the state reserve of supplies;

8) data on a record file managed by special mission units of the Lithuanian

army and entities of operational investigative activities of their officers insured with state social insurance and data on the funds of the aforementioned entities allocated for the state social insurance contributions and income tax contributions of officers thereof;

9) detailed data on the organisation and tactics of transportation of special cargoes;

10) detailed data on the provision of the Lithuanian army, institutions of the national defence system, institutions of the system of the Interior and entities of operational investigative activities with communication equipment and the procedure for using radio frequencies and call signs;

11) data on the inspection and verification of banks and other credit institutions, insurance undertakings, insurance brokers and the undertakings organising lotteries and gaming;

12) projects of fixing exchange rates of the national and base currency and data on the participants of the repurchase transactions executed by the Bank of Lithuania, parties to fixed-term deposits, participants of securities auctions of the Government and the Bank of Lithuania and their bids, liquidity loans;

13) information submitted in proposals of financial institutions on state borrowing in foreign and domestic capital markets and the application of financial derivatives;

14) consolidated detailed data on the organisation and implementation of guarding of the state border and related plans;

15) detailed plans of the organisational and technical development of the Lithuanian army, types thereof, other institutions of the national defence system and the armed forces;

16) consolidated detailed data on the provision of the Lithuanian army, other institutions of the national defence system and the armed forces, institutions of the system of the Interior, entities of operational investigative activities and the Weaponry Fund with weapons, firearms, explosives, combat equipment, special means as well as information on the provision of entities of operational investigative activities with the technical equipment of operational investigative activities;

17) detailed data on programmes and plans of production of weapons, firearms, explosives, combat equipment, special means, the technical equipment of operational investigative activities;

18) detailed data on funds of entities of operational investigative activities and expenditure on the carrying out of the operational investigative activities, and procurement of weapons, firearms, explosives, combat equipment, special means and the technical equipment of operational investigative activities;

19) detailed data on the weapons, firearms, explosives, combat equipment, special means, technical means of operational investigative activities of institutions of the national defence system, institutions of the system of the Interior, entities of operational investigative activities, the Prosecutor' s Office, the Bank of Lithuania, the Weaponry Fund as well as rules for storing and accounting of personal safety and active defence, radiation and chemical safety, special decontamination means and engineering equipment, distribution and organisation of protection thereof;

20) detailed data on the organisation and course of the operational investigative activities of entities of operational investigative activities, the use of measures and methods, tasks, operations, financing thereof, results, logistical support, the information obtained in the course of operational investigative actions, where this information is not assigned to state secrets, as well as the analytical information prepared by entities of operational investigative activities and making use of the information obtained in the course of operational investigative actions;

21) the Republic of Lithuania topographic maps specifying characteristics of strategic objects, characteristics and purpose of military and state border guard objects as well as military purpose maps;

22) conclusion of a polygraph test and sound and/or image recordings made during the test;

23) (repealed as of 1 May 2004);

24) information on conclusion of the contracts concerning privatisation of the undertakings referred to in paragraph 1 of Article 3 and paragraph 1 of Article 4 of the Law on Enterprises and Facilities of Strategic Importance to National Security and Other Enterprises Important in Ensuring National Security, where disclosure of such information would cause prejudice to state economic and political interests;

25) the information prepared by state institutions on the personal and professional characteristics of a candidate for the position of a diplomatic representative of the Republic of Lithuania which influence the taking of a

decision on his appointment.

3. The classified information referred to in paragraph 1 of this Article may be classified as an official secret by a decision of the originator of information, where according to its contents and the amount of the prejudice likely to be caused to the State upon a compromise or loss thereof, such information does not require a higher classification.

4. Entities of secrets shall, on the basis of the list of categories of classified information, draw up detailed lists of the classified information related to their activities. The detailed lists of classified information must provide for classifications of classified information, time periods for classification or conditions of declassification of such information. The detailed lists of the classified information shall be approved and amended by heads of entities of secrets upon agreement with the Commission for Secrets Protection Co-ordination.

Article 8. Time Periods for Classification

Article 8. Time Periods for Classification

1. Information shall be classified for the following time periods:

1) the information classified “Top Secret” for a time period of 30 years, and the information assisting in the identification of covert intelligence staff members, the persons engaged in covert co-operation with intelligence services and covert participants in operational investigative activities as well as the questionnaire data of witnesses or victims classified in the course of criminal proceedings for a time period of 75 years;

2) the information classified “Secret” for a time period of 15 years;

3) the information classified “Confidential” for a time period of 10 years;

4) the information classified “Restricted” for a time period of 5 years.

2. The time period for classification of information shall start from the date of application of a classification.

3. In the cases where it is expedient to classify information for a shorter period for classification than the one specified in paragraph 1 of this Article, the period for classification shall be entered next to the classification.

4. In the cases where classification of information is expedient only until a certain event upon taking place whereof classification of information ceases to be relevant, a specific event or other conditions of declassification of the information shall be specified next to the classification.

5. In the cases where a specific time period for classification cannot be established, although it is known that it is inexpedient to keep information classified during the whole period of classification as established by law or to automatically declassify it upon the expiry of the time period for classification as laid down by law or it is known that the classification of the classified information is going to be changed, the reference "ISS" ("declassified by a decision of an entity") shall be entered next to the classification by a decision of the originator of information.

6. In the cases where the time period for classification of the information comprising a state secret must be longer than the one referred to in subparagraphs 1 and 2 of paragraph 1 of this Article, a decision on the issue shall be taken and the time period for classification shall be extended by the Commission for Secrets Protection Co-ordination upon recommendation of an entity of secrets. The time period for classification may be extended for up to 10 years. The number of extensions shall not be restricted.

7. In the cases where the time period for classification of the information comprising an official secret must be longer than the one referred to in subparagraphs 3 and 4 of paragraph 1 of this Article, a decision on the issue shall be taken and the time period for classification shall be extended by the originator of the classified information. The time period for classification may be extended for up to 5 years. The number of extensions shall not be restricted.

8. The time period for the extension of classification of information shall start from the day of the taking of a decision on the extension of the time period for classification of information.

Article 9. Change of Classifications of Classified Information and Time Periods for Classification

Article 9. Change of Classifications of Classified Information and Time Periods for Classification

1. The originator of classified information shall have the right, in

accordance with the procedure laid down by this Law, to change the affixed classification and the established time period for classification of the information. All entities of secrets whereto the classified information has been passed shall be given written notice of such changes.

2. Where in performing his functions, the recipient of classified information needs to change an assigned classification or a time period for classification, he must, by submitting a justified request, address the originator of classified information. The recipient of classified information may change the assigned classification and the time period for classification only with a written consent of the originator of the information.

Article 10. Declassification of Classified Information

Article 10. Declassification of Classified Information

1. Classified information shall be declassified where:

1) the time period for classification as established in Article 8 of this Law expires;

2) the expediency of classification ceases exist, although the established time period for classification has not expired yet.

2. Where the established time period for classification has not expired yet, classified information may be declassified only by a decision of the originator of classified information.

3. Upon the expiry of the established time period for classification, the information classified “Top Secret”, “Secret” and “Confidential” shall be declassified only by a decision of the originator of the classified information. Upon the expiry of the established time period for classification, the information classified “Restricted” shall be considered declassified without taking a separate decision, where the information has not be assigned an additional reference and the originator of the information has not notified of the extension of the time period for classification of the information.

CHAPTER III

CHAPTER III

COMPETENCE AND POWERS OF STATE INSTITUTIONS IN THE FIELD OF PROTECTION OF CLASSIFIED INFORMATION, RESPONSIBILITY OF INSTITUTIONS AND PERSONS FOR IMPLEMENTATION OF ACTIONS OF THE PROTECTION OF CLASSIFIED INFORMATION

Article 11. Co-ordination of the Protection of Classified Information

Article 11. Co-ordination of the Protection of Classified Information

1. Actions of the protection of the Republic of Lithuania information classified “Top Secret”, “Secret”, “Confidential” and implementation in institutions of the Republic of Lithuania of actions of the protection of the information comprising a secret of other states or international organisations and released to the Republic of Lithuania shall be co-ordinated by a collegial institution the Commission for Secrets Protection Co-ordination. Regulations of the Commission for Secrets Protection Co-ordination shall be approved by the Government. The Commission for Secrets Protection Co-ordination shall have its blank and seal.

2. The Commission for Secrets Protection Co-ordination shall consist of seven members the President of the Republic, the Chairman of the Seimas, the Prime Minister shall each delegated two members. The Chairman of the Commission shall be Director General of the State Security Department.

3. A structural division of the State Security Department which carries out and exercises control over the actions of protection of classified information shall perform functions of the Secretariat of the Commission for Secrets Protection Co-ordination, and the head of this division shall be appointed Secretary of the Commission for Secrets Protection Co-ordination. The Secretariat of the Commission for Secrets Protection Co-ordination shall prepare material for sittings of the Commission for Secrets Protection Co-ordination, implement the decisions taken by the Commission for Secrets Protection Co-ordination and control the implementation thereof in entities of secrets.

4. Members, Secretary and staff of the Secretariat of the Commission for Secrets Protection Co-ordination may be only the persons who have obtained, in

accordance with the procedure laid down by this Law, an authorisation to handle and familiarise with the information classified "Top Secret" as well as a security clearance granting the right to familiarise with the classified information released by other states or international organisation and assigned a classification equivalent to "Top Secret".

5. The Commission for Secrets Protection Co-ordination shall perform the following main functions:

1) co-ordinate the implementation of provisions of the Republic of Lithuania international treaties on reciprocal protection of classified information, where necessary, initiate the conclusion of such treaties or denunciation of concluded treaties;

2) ensure control over the implementation of the actions required for the protection of the classified information assigned the classifications equivalent to "Top Secret", "Secret" and "Confidential" and released to the Republic of Lithuania by foreign states, the European Union or international organisations, perform other functions to ensure the security of the classified information passed to the Republic of Lithuania according to legal acts of the European Union or international treaties of the Republic of Lithuania with the foreign states or international organisations;

3) ensure the organisation of control over the actions of protection of information as provided for in the international treaties of the Republic of Lithuania related to assurance of the protection of classified information and timely implementation thereof in all entities of secrets and structural divisions storing the classified information released to the Republic of Lithuania by foreign states or international organisations;

4) upon the submission of the institutions which have carried out the screening of candidates, issue security clearances to the persons needing, in discharging their official duties, to handle or familiarise with the classified information released to the Republic of Lithuania by foreign states or international organisations and, on the grounds established by this Law, revoke the security clearances;

5) proposes that the State Security Department sets up the national Central Registry to engage in the registration, accounting and distribution of the classified documents released to the Republic of Lithuania by foreign states, the European Union or international organisations and assigned the classifications equivalent to "Top Secret", "Secret";

6) upon the submission of entities of secrets, take decisions on the expediency of setting up of new registries of the classified information

released to the Republic of Lithuania, recognise established registries as suitable to store the classified information released, take decisions on the expediency of liquidation of the established registries. Where necessary, the Commission shall propose that entities of secrets set up other independent systems of registries of classified information or liquidate them, where required by international treaties or agreements of the Republic of Lithuania;

7) authorise entities of secrets or structural divisions thereof to perform functions of the institutions responsible for the implementation of international treaties on the protection of classified information;

8) submit proposals on the improvement or repeal of this Law and other legal acts related to the protection of classified information, improvement of the system of legal regulation of classified information protection which is currently in force;

9) set general requirements for specific fields of the protection of classified information (personnel security, physical security, security of classified contracts, administration of the classified documents released to the Republic of Lithuania by foreign states or international organisations), provide entities of secrets with interpretations on issues of the protection of classified information;

10) examine the detailed lists drawn up by entities of secrets and containing the classified information related to activities thereof as well as amendments to the said lists and submit proposals and notes thereon to entities of secrets;

11) through the mediation of entities of secrets, decide issues on the possibility to issue security clearances or authorisations to handle or familiarise with classified information to the persons having double citizenship or the persons not meeting the qualification of permanent residence in the Republic of Lithuania referred to in subparagraph 2 of paragraph 2 of Article 16 of this Law;

12) upon the expiry of the time period for classification of information as established in subparagraphs 1 and 2 of paragraph 1 of Article 8 of this Law and upon the submission of entities of secrets, decide issues on the expedience of extension of the time period for classification;

13) solve disputes between entities of secrets as well as disputes between entities of secrets and other persons rising in respect of classification of information, storage, use, declassification, control of the protection of classified information and in respect of the validity of denial or revocation

of authorisations to handle or familiarise with classified information as well as security clearances and facility security clearances;

14) submit proposals to entities of secrets on the lawfulness of acquisition of the information which, according to its nature and importance, should be classified, but belongs by the right of ownership to an entity of secrets that is not a natural or legal person and the amount of a possible recompense to the holder of the information;

15) upon the submission of entities of secrets, decide issues on the possibility to release the information comprising a state secret to other states or international organisations wherewith no international treaties have been concluded on the reciprocal protection of classified information;

16) establish forms of a person' s, contractor' s (sub-contractor' s) consent for inspection, an authorisation to handle or familiarise with classified information, a security clearance and certificate confirming the issuance of this clearance, a questionnaire to obtain an authorisation to handle or familiarise with classified information, pledge of a person to protect classified information, classified contracts security questionnaire, a facility security clearance.

6. The Commission for Secrets Protection Co-ordination shall seek to ensure that the information of the same importance in different entities of secrets be assigned the same classification and established the same level of protection.

7. The decisions taken by the Commission for Secrets Protection Co-ordination in performing the functions referred to in subparagraphs 13, 1013, 1516 of paragraph 5 of this Article shall be binding on entities of secrets.

Article 12. Implementation of the Protection of Classified Information

Article 12. Implementation of the Protection of Classified Information

1. The policy of the protection of classified information shall be formulated by the Government and the Commission for Secrets Protection Co-ordination. The protection of classified information shall be organised and implemented by entities of secrets in accordance with the procedure laid down by this Law, the Government, the Commission for Secrets Protection Co-ordination, the institutions performing functions of the Security Accreditation Authority, the

National Communications Security Authority, the National Distribution Authority as well as the institutions ensuring the security of classified contracts.

2. The head of an entity of secrets shall be responsible for an overall organisation and condition of the protection of the classified information at the disposal of the entity of secrets. Heads of structural divisions, the persons authorised by them as well as the persons whereto information has been entrusted shall be responsible for the carrying out of requirements for the protection of classified information in the structural divisions of an entity of secrets wherein the classified information is stored or used. A person entrusted with classified information shall be directly liable for a loss or compromise of the said information.

3. Entities of secrets shall draw up and approve lists of the structural divisions which handle classified information or store the information classified “Top Secret”, “Secret” or “Confidential” and ensure that the classified information is used and stored only by the structural divisions entered in the lists.

4. Entities of secrets shall draw up lists of the positions subject to authorisations to handle or familiarise with classified information.

5. Entities of secrets shall draw up lists of the positions subject to security clearances.

6. The lists of positions referred to in paragraphs 4 and 5 of this Article must specify the highest category of classified information which the persons occupying the positions specified in a list may handle or familiarise with.

7. The persons in charge of the physical security of the information classified “Top Secret”, “Secret” or “Confidential” or authorised to transport the said information must hold authorisations to handle or familiarise with the information classified “Secret”.

8. In the entities of secrets or structural divisions thereof housing the classified information of the Republic of Lithuania, foreign states or international organisations, lists of the persons who have been issued authorisations to handle or familiarise with classified information or holding security clearances must be drawn up.

Article 13. Special Commission of Experts

Article 13. Special Commission of Experts

1. In entities of secrets, the protection of classified information shall be co-ordinated by the special standing commissions of experts formed by a decision of the head of an entity of secrets. They shall:

1) draft the legal acts of the entity of secrets related to the protection of classified information and supervise the implementation of these legal acts;

2) submit proposals to an entity of secrets on the issuance to persons of authorisations to handle or familiarise with classified information or revocation of issued authorisations;

3) submit proposals and conclusions on the validity of classification of information, changing of classifications, declassification or destruction of classified information;

4) organise checks of the condition of protection of the classified information at the disposal of an entity of secrets and submit proposals on the prevention of breaches of requirements for the protection of classified information, deal with other issues related to the protection of classified information.

2. Taking into consideration the volume of classified information, the head of an entity of secrets shall be permitted not to form a special commission of experts and to assign the performance of its functions to an authorised person.

3. Only the persons who have obtained, in accordance with the procedure laid down by this Law, an authorisation to handle or familiarise with classified information or, where an entity of secrets uses the classified information prepared by foreign states or international organisations, a security clearance may be members of a special commission of experts. The authorisations of the special commission of experts to handle or familiarise with classified information or the security clearances must be commensurate with the highest classification of the information at the disposal of the entity of secrets.

Article 14. Duty to Appoint a Responsible Person

Article 14. Duty to Appoint a Responsible Person

By a decision of an entity of secrets or a person authorised by it or the head of the contractor (sub-contractor), a person must be appointed to be responsible for organisation and implementation of the administration, protection and control of the classified information at the disposal of the entity of secrets or the contractor (sub-contractor).

CHAPTER IV PERSONNEL SECURITY

CHAPTER IV PERSONNEL SECURITY

Article 15. Authorisation to Handle or Familiarise with Classified Information and a Security Clearance

Article 15. Authorisation to Handle or Familiarise with Classified Information and a Security Clearance

1. A position related to the use of the information of the Republic of Lithuania classified “Top Secret”, “Secret” or “Confidential” or to the protection of the said information shall be subject to appropriate authorisations to handle or familiarise with classified information. A position related to the use of the classified information of foreign states or international organisations assigned the classifications equivalent to “Top Secret”, “Secret” or “Confidential” or to the protection of the said information shall be subject to appropriate security clearances. The candidates selected for a position related to the use of classified information or to protection thereof may be appointed for the position upon prior screening of their candidacies and obtaining of a conclusion that the person meets the conditions referred to in paragraph 1 of Article 16 of this Article.

2. The position occupied by the President of the Republic, the Chairman of the Seimas and the Prime Minister shall entitle them to familiarise with classified information and to use it.

3. In the course of a pre-trial investigation or hearing a criminal case the file whereof contains classified information, the suspect (the accused) and counsel for the defence of the suspect (the accused) shall have the right, in accordance with the procedure laid down by the Code on Criminal Proceedings, to familiarise with the classified information contained in the file, except for the data assisting in the identification of a victim or witness who has been granted anonymity.

4. The persons listed in paragraph 3 of this Article shall, prior to granting to them the right to familiarise with classified information, be warned of criminal liability for a disclosure of classified information. The persons listed in paragraphs 5 and 6 of this Article must, prior to issuing to them a temporary authorisation to handle or familiarise with the classified information of the Republic of Lithuania, foreign states or international organisations, submit a written pledge of the set form to protect the classified information entrusted to them.

5. Upon the declaration in the Republic of Lithuania of a state of war or emergency or in the course of military operations and by a decision of the head of an entity of secrets or a person authorised by him, a person who does not hold an authorisation to handle classified information may be granted the right to familiarise with it, where such information is needed for the performance of the functions or carrying out of the tasks assigned to him.

6. In the exceptional cases as specified in the NATO regulatory documents regulating the protection of classified information, the head of an entity of secrets may issue to a person who does not hold a security clearance a written temporary authorisation to familiarise with the classified information released to Lithuania by NATO, where the loyalty of the person to the State of Lithuania and his security cast no doubt. The authorisation issued by the head of the entity of secrets must specify the type of the classified information which the person is granted the right to familiarise with.

7. Entities of secrets may issue authorisations to handle or familiarise with classified information only subject to a conclusion of the State Security Department that a person meets the conditions referred to in paragraph 1 of Article 16 of this Law. This provision shall not be applied to the issuance of authorisations to the persons referred in subparagraph 4 of paragraph 3 of Article 17 of this Law.

8. A decision on the issuance of a security clearance shall be taken by the Commission for Secrets Protection Co-ordination in accordance with the procedure laid down by this Law.

Article 16. Conditions of the Issuance of an Authorisation to Handle or Familiarise with Classified Information and a Security Clearance

Article 16. Conditions of the Issuance of an Authorisation to Handle or

Familiarise with Classified Information and a Security Clearance

1. A person applying for an authorisation to handle or familiarise with classified information or for a security clearance shall be issued the said authorisation or clearance, where:

1) the person is a citizen of the Republic of Lithuania;

2) the person submits a completed questionnaire of the set form and provides a written consent for screening of his candidacy;

3) the person pledges in writing to protect classified information;

4) the facts collected in the course of the screening cast no doubt as to the person’ s security or loyalty to the State of Lithuania;

5) the screening does not establish any circumstance referred to in paragraph 2 of this Article.

2. An authorisation to handle or familiarise with classified information or a security clearance shall not be issued to a person, where the person:

1) does not meet at least one condition referred to in paragraph 1 of this Article;

2) has permanently resided in the Republic of Lithuania for less than last 5 years, and the Commission for Secrets Protection Co-ordination has, in accordance with the procedure laid down in subparagraph 11 of paragraph 5 of Article 11 of this Law, taken a decision not to issue an authorisation to handle or familiarise with classified information or a security clearance;

3) has applied to appropriate state institutions for renunciation of the citizenship of the Republic of Lithuania;

4) has double citizenship, and the Commission for Secrets Protection Co-ordination has, in accordance with the procedure laid down in subparagraph 11 of paragraph 5 of Article 11 of this Law, taken a decision not to issue an authorisation to handle or familiarise with classified information or a security clearance;

5) has been convicted for a crime against the independence of the State of Lithuania, territorial integrity and constitutional order thereof or for any particularly serious crime or a criminal act related to the seizure of an official secret, other unauthorised acquisition or compromise;

6) has a record of conviction for a serious or less serious crime;

7) has been recognised incompetent or of limited competence in accordance with the procedure laid down by laws;

8) has collaborated with or maintains relations with a special service of another state or with the persons collaborating with the special service of another state due to the interests hostile to the Republic of Lithuania;

9) maintains relations with the persons belonging to organised criminal groups or criminal associations;

10) takes part in the activities of a non-registered religious community, political organisation or formations thereof;

11) deliberately concealed from or submitted to the institutions screening his candidacy false biographical facts or other personal data, the data on his connections and surroundings likely to influence a decision on the issuance of an authorisation to handle or familiarise with classified information or a security clearance;

12) has been dismissed for a violation of the procedure for handling classified information in accordance with the procedure laid down by laws or other legal acts or where an authorisation to handle classified information or a security clearance has been revoked for such violations;

13) is being prosecuted for an intentional criminal act or is subject to a pre-trial investigation or operational investigation related to the said act;

14) is subject to the application of preventive measures in accordance with the Law on Organised Crime Prevention;

15) receives income from military or special services of other states, where this is not provided for in international treaties or agreements of the Republic of Lithuania;

16) cannot prove the lawfulness of acquisition of the property which he manages, uses or has at his disposal, and where his standard of living does not correspond to actual income;

17) abuses alcohol, consumes narcotic, psychotropic or other substances with psychological effects or where other personal and professional properties due to which he is not suitable for handling classified information are established;

18) suffers from mental disorders or other health disorders which may limit his capabilities and negatively influence his actions.

3. The persons holding authorisations or security clearances granting the right to handle or familiarise with the information applied a higher classification shall not need a separate authorisation or a security clearance to handle or familiarise themselves with the information applied a lower classification.

4. Where a person needs to handle or familiarise with the information applied a higher classification than specified in an authorisation or a security clearance issued to him, his candidacy shall be screened anew.

5. A security clearance and an authorisation to handle or familiarise with the information classified "Top Secret" shall be issued for a time period not exceeding five years, and that to handle or familiarise with the information classified "Secret", "Confidential" for a time period not exceeding ten years. This time period shall start from the date of signing the consent of the State Security Department to issue the said authorisation or from the date of submission of a conclusion of an institution which has carried out the screening of a candidacy, where the authorisation to handle or familiarise with classified information or the security clearance is issued to covert participants in operational investigative activities, covert intelligence staff members and the persons engaged in covert co-operation with intelligence services.

6. Additional screening of a person shall be carried out six months prior to the expiry of validity of an authorisation to handle or familiarise with classified information or a security clearance. The person may also be subject to repeated screening prior to the expiry of the time periods established by this Article, where the circumstances provided for in paragraph 2 of this Article are suspected to have arisen. In the course of the repeated screening and by a decision of an entity of secrets, the person may be prohibited from handling classified information.

7. A decision on the denial of an authorisation to handle or familiarise with classified information, the denial of a security clearance, an objection of the State Security Department on the issuance to a person of the said authorisation as well as a decision of the institutions screening the candidacy to terminate the screening of the candidacy upon the establishment of the circumstances referred to in paragraph 2 of this Article may be appealed against by the person or an entity of secrets to the Commission for Secrets Protection Co-ordination within 30 working days of the receipt of the decision. Where necessary, the Commission shall require the institutions which

have carried out the screening of the candidacy to collect and submit additional data on the person. A decision of the Commission for Secrets Protection Co-ordination shall be binding on the entity of secrets.

8. The persons whose duties involve the use of the information comprising an official secret and classified "Restricted" or the protection thereof shall be granted the right to handle or familiarise with the said information by an entity of secrets. The consent of the State Security Department shall not be required. The procedure for granting of the right to handle or familiarise with such information shall be laid down by entities of secrets on the basis of the basic principles approved by the Commission for Secrets Protection Co-ordination.

Article 17. Screening of a Person's Candidacy

Article 17. Screening of a Person's Candidacy

1. The main aim of screening of a person's candidacy shall be to determine whether the person applying for an authorisation to handle or familiarise with classified information or for a security clearance may be entrusted with the classified information and whether the person subject to screening is secure and loyal to the State of Lithuania. Candidacies shall be screened upon the submission of an entity of secrets or a person authorised by it.

2. A person applying for an authorisation to handle or familiarise with classified information or for a security clearance shall submit to a responsible person a completed questionnaire of the set form and a written consent for screening. The person shall also submit a detailed autobiography, where he applies for an authorisation to handle or familiarise with the information classified "Top Secret" or "Secret". Screening of a candidacy shall aim at establishing whether there are any conditions referred to in paragraph 2 of Article 16 of this Law. In the course of the screening, methods and measures of operational investigative activities may not be employed, with the exception of an intelligence interview and review of the operational record file data. Prior to taking a decision, the institutions screening a candidacy may invite a person for an interview, require the person's written clarifications and, where necessary and subject to the person's consent, perform a polygraph test.

3. Candidacies of the persons applying for an authorisation to handle or familiarise with classified information shall be screened:

1) in respect of the persons employed or applying for employment in the

national defence system by the Second Investigation Department under the Ministry of National Defence and the State Security Department;

2) in respect of the persons employed or applying for employment in the system of the Interior by the institutions authorised by the Minister of the Interior and the State Security Department;

3) in respect of the persons employed or applying for employment in the Special Investigation Service by the Special Investigation Service and the State Security Department;

4) in respect of covert participants in operational investigative activities, covert intelligence staff members and the persons engaged in covert co-operation with intelligence services by entities of secrets;

5) by the State Security Department, where an authorisation to handle or familiarise with classified information or a security clearance has been applied for by a person not specified in subparagraphs 1-4 of this paragraph.

4. Where a candidacy has been screened by the Second Investigation Department under the Ministry of National Defence, the institutions authorised by the Minister of the Interior or the Special Investigation Service and where no circumstances referred to in paragraph 2 of Article 16 of this Law were established in the course of the screening, a questionnaire completed by the person, his autobiography and conclusions of the screening carried out shall be submitted to the State Security Department. The State Security Department shall assess the results of the screening according to the information which is at its disposal and shall, where necessary, collect additional information or recommend this to be done by the institutions which have carried out the screening of the candidacy and submit to an entity of secrets a consent or a reasoned objection with regard to the possibility of issuing to the person an authorisation of a relevant category to handle or familiarise with classified information.

5. In the cases where a candidacy has been screened by the Second Investigation Department under the Ministry of National Defence, the institutions authorised by the Minister of the Interior or the Special Investigation Service and where the circumstances referred to in paragraph 2 of Article 16 of this Law were established in the course of the screening, the screening shall be terminated by a decision of the Minister of National Defence or the Minister of the Interior or the persons authorised by them or Director of the Special Investigation Service. The decision shall be notified to an entity of secrets and the person candidacy whereof was subject to screening. The State Security Department shall not screen the candidacy.

6. The candidacy of a person applying for a security clearance shall be screened by the State Security Department. Where the person holds an authorisation to handle or familiarise with classified information issued not earlier than 18 months ago, the State Security Department shall submit to the Commission for Secrets Protection Co-ordination the material on the basis whereof the person has been issued the authorisation. It shall be possible not to screen the candidacy anew.

7. The institutions carrying out screening must screen the candidacy of a person applying for an authorisation to handle or familiarise with classified information or for a security clearance:

1) within 60 working days, where the person is applying for an authorisation to handle or familiarise with the information classified "Confidential " or for an appropriate security clearance;

2) within 90 working days, where the person is applying for an authorisation to handle or familiarise with the information classified "Secret" or for an appropriate security clearance;

3) within 120 working days, where the person is applying for an authorisation to handle or familiarise with the information classified "Top Secret" or for an appropriate security clearance.

8. Where the State Security Department consents to the issuance to a person of an authorisation to handle or familiarise with classified information, an entity of secrets shall issue an authorisation of the set form to handle or familiarise with classified information.

9. A decision on the issuance of an authorisation to handle or familiarise with the information applied an appropriate classification must be taken by an entity of secrets within 20 working days of signing of the consent of the State Security Department to issue the said authorisation. The entity of secrets must notify the State Security Department of the authorisations issued to handle or familiarise with classified information within 10 working days.

10. An authorisation to handle or familiarise with classified information as issued to a person by an entity of secrets together with a written pledge of the person to protect classified information shall be kept in the person's file or in accordance with the procedure laid down by the entity of secrets.

11. Security clearances shall be registered and stored in accordance with the procedure laid down by the Commission for Secrets Protection Co-ordination.

12. Upon the request of appropriate institutions of foreign states or international organisations, the Commission for Secrets Protection Co-ordination or entities of secrets shall submit certificates of the form set by the Commission for Secrets Protection Co-ordination confirming that a person has been issued a security clearance.

13. The institutions carrying out screening of a candidacy shall have the right to obtain information on a person subject to screening from all state and municipal institutions, banks and other legal persons.

Article 18. Revocation of an Authorisation to Handle or Familiarise with Classified Information and a Security Clearance

Article 18. Revocation of an Authorisation to Handle or Familiarise with Classified Information and a Security Clearance

1. An authorisation to handle or familiarise with classified information and a security clearance shall be revoked, where:

1) a person renounces or loses the citizenship of the Republic of Lithuania;

2) a person has on repeated occasions violated the procedure laid down for handling classified information, or where, due to a grave breach of this procedure, a threat has arisen of a loss or compromise of classified information;

3) employment (service) relations are terminated with an entity of secrets or powers of the persons elected or appointed expire;

4) any of the circumstances referred to in paragraph 2 of Article 16 of this Law arises or transpires.

2. An entity of secrets shall, on its own initiative or upon a reasoned recommendation of the State Security Department, revoke an authorisation to handle or familiarise with classified information. The entity of secrets shall give written notice of a decision taken on the revocation of the authorisation to handle or familiarise with classified information to the State Security Department within 10 working days.

3. Upon the request of a person whose authorisation to handle or familiarise

with classified information or security clearance has been revoked, an entity of secrets must provide a written specification of the reasons for revocation of the authorisation to handle or familiarise with classified information.

4. The Commission for Secrets Protection Co-ordination shall revoke a security clearance on its own initiative or upon a reasoned recommendation of the State Security Department or an entity of secrets.

5. Upon the receipt of a reasoned recommendation of the State Security Department on the revocation of an authorisation, a person or an entity of secrets shall have the right to appeal against a decision on the revocation of an authorisation to handle or familiarise with classified information or a security clearance to the Commission for Secrets Protection Co-ordination within 30 working days of the receipt of the decision. Where necessary, this commission shall require the institutions which have carried out the screening of a candidacy to collect and submit additional data on the person. The decision of the Commission for Secrets Protection Co-ordination shall be binding on the entity of secrets.

6. The revocation of an authorisation to handle or familiarise with classified information or a security clearance shall not relieve a person from the obligation not to disclose the classified information obtained in the course of service as well as from liability for a disclosure of such information.

Article 19. Duties of a Person Holding an Authorisation to Handle or Familiarise with Classified Information or a Security Clearance

Article 19. Duties of a Person Holding an Authorisation to Handle or Familiarise with Classified Information or a Security Clearance

A person holding an authorisation to handle or familiarise with classified information or a security clearance shall be under an obligation:

1) to know requirements of the legal acts regulating the protection of classified information and carry them out;

2) not to disclose, lose and release the classified information entrusted to or obtained by him to unauthorised persons as well as to the persons who, although having the right to handle classified information, are not authorised to familiarise with it;

3) to protect the classified information entrusted to him or obtained during the period of service for the entire time period for classification of this information;

4) to act on a need-to-know basis;

5) to prevent the unlawful actions of third parties which may result in a disclosure, loss, seizure or other unauthorised acquisition of classified information and to immediately notify of these facts and other circumstances of a disclosure or loss of classified information a responsible person or the head of an entity of secrets;

6) to immediately notify a responsible person of a loss or disclosure of the classified information entrusted to him as well as of breaches of requirements for the protection of classified information;

7) when terminating employment (service) relations, being transferred to a position not involving to the use of classified information, to return all the classified information entrusted to him to a responsible person;

8) to provide information, oral or written clarifications to the persons authorised to exercise control of the protection of classified information;

9) to notify a responsible person of changes in the questionnaire data submitted to the institutions which have screened his candidacy;

10) six months prior to the expiry of validity of an authorisation to handle or familiarise with classified information or a security clearance as well as in the course of additional screening carried out by authorised institutions, to submit to a responsible person the documents required for the carrying out of the screening.

Article 20. Functions of a Responsible Person in the Field of Personnel Security

Article 20. Functions of a Responsible Person in the Field of Personnel Security

A responsible person shall:

1) organise the issuance of authorisations to handle or familiarise with classified information and keep accounts thereof;

2) ensure that classified information is accessed only by authorised persons and that the need-to-know principle is strictly complied with;

3) ensure that the classification applied to the classified information which a person handles or familiarises with is not higher than the one specified in an authorisation issued to the person;

4) control that all the persons handling or familiarising with classified information carry out requirements of the legal acts regulating the protection of classified information;

5) inform the institutions screening a candidacy of changes in a person's questionnaire data likely to influence the issuance or revocation of an authorisation;

6) six months prior to the expiry of validity of an authorisation to handle or familiarise with the information comprising a state secret or of a security clearance, organise repeated screening of a candidacy;

7) collect from the persons who are issued authorisations to handle or familiarise with classified information written pledges of the set form to protect classified information;

8) familiarise persons, against their signature, with a detailed list of the classified information related to activities of an entity of secrets;

9) once per calendar year, inform the persons entrusted with classified information of statutory liability for unauthorised holding of classified information, compromise, loss, seizure or other unauthorised acquisition of classified information;

10) once per calendar year, familiarise the persons employed on duties related to the use or protection of classified information, against their signature, with requirements of the legal acts regulating the protection of classified information.

CHAPTER V ADMINISTRATION OF CLASSIFIED INFORMATION

CHAPTER V ADMINISTRATION OF CLASSIFIED INFORMATION

Article 21. Application of a Classification to a Document or Part Thereof

Article 21. Application of a Classification to a Document or Part Thereof

1. The head of an entity of secrets' structural division which has drafted a document shall consider a proposal of the person who has drafted the document and take a decision on the application of a classification to the document and the establishment of a time period for classification thereof and be liable for the validity of the decision taken.

2. A document shall not be applied a classification solely for the reason of its topic or the classification of a document in reply to which it has been drafted.

3. The classification of a document shall be determined according to the highest classification of the information contained in the text of the document.

4. Where a document consists of separate parts each applied a different classification or contains annexes whose classifications are different from the classification of the document, clear references must be provided in the document about different classifications of the parts of the document and annexes thereto in the text of the document, listing of the annexes or a list of the parts of the document (contents) as well as at the beginning of the said parts of the document's text or on the annexes to the document.

5. Where parts of or annexes to a document are integral part of the document, the said document shall be included in the accounting records of classified documents and stored according to its most highly classified part or annexes. The parts of the document or annexes thereto which may be detached shall be distributed, entered in accounting records and stored according to the classification of the said parts of the document or annexes thereto.

Article 22. Requirements for the Administration of Classified Documents

Article 22. Requirements for the Administration of Classified Documents

1. The documents classified "Top Secret" shall be administered in the

following manner:

1) handled and stored in Class I or Class II security areas;

2) conveyed to the recipient of classified information against his signature;

3) may not be copied;

4) conveyed to executors against their signature by recording the fact of the conveyance in classified information registration media;

5) released by the recipient of classified information to another entity of secrets only with a written consent of the originator of the information;

6) must contain attached lists of the persons familiarised with the contents of a document;

7) stored separately from the documents which have been applied other classifications, with the exception of the documents stored in computer storage media;

8) may not be destroyed a document no longer needed shall be returned to the originator of information, with the exception of the cases referred to in Article 26 of this Law.

2. The documents classified "Secret" shall be administered in the following manner:

1) handled and stored in Class I or Class II security areas;

2) conveyed to the recipient of classified information against his signature;

3) may be reproduced or copied only subject to a written decision of the head of an entity of secrets or a person authorised by him and with a written consent of the originator of the information;

4) copies shall be registered and numbered;

5) may be released by the recipient of classified information to another entity of secrets only with a written consent of the originator of the information;

6) conveyed to executors against their signature by recording the fact of the conveyance in classified information registration media;

7) destroyed (including copies thereof) upon issuing destruction certificates.

3. The documents classified “Confidential” shall be administered in the following manner:

1) handled and stored in Class I or Class II security areas;

2) may be reproduced or copied by a decision of a person exercising control over the execution of a document and in compliance with the need-to-know principle, where the document does not bear the reference “Subject to a consent of the originator of information”. Copies must be registered and numbered;

3) conveyed to executors against their signature by recording the fact of the conveyance in classified information registration media;

4) destroyed (including copies thereof) upon issuing destruction certificates.

4. The documents classified “Restricted” shall be administered in the following manner:

1) handled and stored in an administrative security area;

2) may be distributed, reproduced, copied and, in compliance with the need-to-know principle, released to third parties for familiarisation by a decision of the executor, where a document does not bear the reference “Subject to a consent of the originator of information”.

5. The procedure for distributing, reproducing, destroying of the documents classified “Restricted” or familiarising third parties with contents thereof may be laid down by entities of secrets.

Article 23. Familiarisation with the Classified Information at the Disposal of Another Entity of Secrets

Article 23. Familiarisation with the Classified Information at the Disposal of Another Entity of Secrets

1. The right to familiarise with the information classified “Top Secret”, “Secret” or “Confidential” and being at the disposal of another entity of

secrets shall be granted to a person by the head of the entity of secrets having the information at its disposal in compliance the need-to-know principle. The person must submit a letter of targeted authorisation of the head of an institution where he is employed. The letter of targeted authorisation must confirm that the person holds an authorisation to handle or familiarise with the classified information applied an appropriate classification or a security clearance, where it is necessary to familiarise with the classified information released by a foreign state or an international organisation, and specify the need, as based on the discharge of immediate duties, to familiarise with specific classified information as well as the volume of the classified information which the person needs to familiarise with.

2. Where a decision is taken not to permit a person to familiarise with the classified information specified in a letter of targeted authorisation, the head of an entity of secrets having this information at its disposal must provide reasons for his decision and, within 10 working days, familiarise with the decision the head of an institution which has provided the person with the letter of targeted authorisation. The said decision may be appealed against to the Commission for Secrets Protection Co-ordination, which shall take a decision binding on the entity of secrets.

Article 24. Transportation of Classified Information

Article 24. Transportation of Classified Information

1. The documents, products and other objects classified “Top Secret” and “Secret” must be conveyed by diplomatic, military couriers or couriers of the courier services to which special powers have been granted, where they are armed with firearms, or by the persons authorised by a entity of secrets.

2. The documents, products and other objects classified “Confidential” and “Restricted” may be conveyed by the persons listed in paragraph 1 of this Article or couriers of courier services.

3. The persons carrying classified documents, products and other objects must:

1) ensure the security of the documents, products and other objects conveyed;

2) carry the documents, products and other objects so that unauthorised persons could not identify that classified information is being carried or familiarise with the contents of the said information.

4. The recipient of classified information must acknowledge receipt of the documents, products and other objects classified “Top Secret” and “Secret” with his signature.

5. The persons carrying classified documents, products and other objects shall be prohibited from familiarising with classified information.

6. A person carrying classified documents, products and other objects must ensure their protection against loss by any means combat actions, available special means or a firearm. These means must be commensurate with an occurrence or imminent threat of a seizure of classified information.

7. Classified documents, products and other objects shall be carried by selecting the safest route and mode of transportation.

Article 25. Destruction of Classified Information

Article 25. Destruction of Classified Information

1. Classified information shall be destroyed in accordance with the procedure laid down by the Government.

2. A decision on the destruction of classified information shall be taken by the head of an entity of secrets or a person authorised by him, with the exception of the cases referred to in subparagraph 8 of paragraph 1 of Article 22 of this Law.

3. Classified information must be destroyed so that contents of the classified information or part thereof could not be reconstituted.

Article 26. Evacuation or Destruction of Classified Information in the Event of a State of War or Emergency

Article 26. Evacuation or Destruction of Classified Information in the Event of a State of War or Emergency

1. An entity of secrets handling or storing classified information must prepare and approve plans of the evacuation or destruction of classified

information in the event of a state of war or emergency.

2. Plans must lay down the procedure for evacuating or destroying classified information in the event of an actual threat of a loss or disclosure of classified information. The classified information which has been applied a higher classification shall be evacuated or destroyed first.

Article 27. Inspection of Classified Information

Article 27. Inspection of Classified Information

1. Once annually, the persons authorised by the head of an entity of secrets must inspect the information comprising a state secret. Conclusions of the inspection shall be documented in a statement. The statement shall be approved by the head of the entity of secrets.

2. Once per three years, the persons authorised by the head of an entity of secrets must inspect the information classified “Confidential”. Conclusions of the inspection shall be formalised by a statement. The statement shall be approved by the head of the entity of secrets.

3. The periodicity of inspecting the information classified “Restricted” shall be established by an entity of secrets.

4. The aim of inspections shall be to establish whether classified information has not be lost or corrupted.

5. It shall be considered that classified information has been accounted for, where:

1) a classified document, product or other object may be viewed;

2) receipt of information has been confirmed in writing by an appropriate entity of secrets or a structural division whereto classified information has been released;

3) destruction thereof has been recorded in accordance with the procedure laid down by legal acts;

4) an appropriate notification has been given or decision has been taken on the declassification of information.

Article 28. Functions of a Responsible Person in the Field of Administration of Classified Information

Article 28. Functions of a Responsible Person in the Field of Administration of Classified Information

A responsible person shall:

1) organise the accounting of classified information, control distribution and manage registration thereof;

2) select information for destruction, declassification or extension of a time period for classification of the said information;

3) be responsible for managing classified information registration media;

4) be responsible for conveyance of classified information to executors and other entities of secrets;

5) be responsible for a timely notification of entities of secrets of changes in the classifications, declassification or extension of a time period for classification of classified information;

6) by a decision of the head of an entity of secrets or a person authorised by him, familiarise the persons authorised by other entities of secrets with the information classified “Top Secret”, “Secret” or “Confidential”;

7) organise, at the intervals established in Article 27 of this Law, the inspection of classified information;

8) organise the process of destruction of classified information.

Article 29. Regulation of the Administration of Classified Information

Article 29. Regulation of the Administration of Classified Information

A detailed procedure for preparing, documenting, sending, transporting, receiving, reproducing, destroying and accounting of classified information shall be laid down by the Government in compliance with the provisions of

Chapter V of this Law.

CHAPTER VI PHYSICAL SECURITY OF CLASSIFIED INFORMATION

CHAPTER VI PHYSICAL SECURITY OF CLASSIFIED INFORMATION

Article 30. Implementation of Physical Security

Article 30. Implementation of Physical Security

1. Entities of secrets must ensure adequate protection of all territories, premises and workstations in which classified information is handled or stored by relevant physical, mechanical, procedural and electronic security measures and assignment of guards.

2. The physical security measures applied for the protection of classified information must be designed to:

1) deny entry by unauthorised persons of the territories and premises where classified information is handled or stored;

2) deter unauthorised actions of employees and record such actions;

3) prevent the employees who do not hold an authorisation to handle or familiarise with classified information from familiarising with contents of the classified information;

4) record breaches of physical security.

3. In deciding on the selection and installation as well as use of specific means of protection, account shall be taken by an entity of secrets of the following factors:

1) the classification of protected classified information;

2) the nature and volume of protected information;

3) the risk factors security of the persons employed in an entity of secrets, characteristic of the surrounding environment, criminal situation, the

location of a building, layout of premises, size of the territory, likelihood of uncontrolled entry to a protected area, etc.

4. Physical security shall consist of:

1) the establishment of security areas;

2) the installation and use of the mechanical security measures to impede intrusion or forced entry into a territory and premises;

3) the installation and use of security alarms;

4) the installation and use of the electronic surveillance and electronic security measures allowing personal identification and restricting entry as well as recording entry into premises, presence in and exit from the premises;

5) the training, assignment and allocation of guards;

6) the regulation of physical security procedures the internal regulations providing that premises must be unlocked and locked, alarm be switched off and switched on and monitoring of premises and other physical security procedures be carried out.

5. Taking account of the factors listed in paragraph 3 of this Article and facilities of ensuring the protection of protected information, the constituent parts of physical security as referred to in subparagraphs 2-5 of paragraph 4 of this Article may be applied in the aggregate or priority may be given to several or one of them.

Article 31. Security Areas

Article 31. Security Areas

1. The territories and premises in which classified information is handled or stored shall be subdivided into separate security areas according to the classifications applied to the information, mode of storage and risk of unauthorised familiarisation with the classified information.

2. An administrative security area a defined territory and/or premises in which the movement of persons and vehicles shall be controlled. Class I or Class II security areas shall be accessible only from the administrative area. Only the information classified “Restricted” may be stored or handled in the administrative area. The classified information stored in the administrative

security area must be kept in metal cabinets or in safes.

3. Class II security area the territories and premises in which the information classified "Confidential" and above is stored or handled as well as the premises entry into which constitutes direct access to the central control of this security area's electronic security measures. The information stored in Class II security area and classified "Secret" or "Top Secret" must be kept in safes with user-specific combination settings and mechanical locks or in repositories specially designed to store such information. The information stored in Class II security area and classified "Confidential" must be kept in metal cabinets or in safes.

4. Class II security area shall be imposed the following requirements:

1) all entrances to and exits from the area must be established, protected and controlled;

2) the area may be accessed only by the persons holding an authorisation to handle or familiarise with the information classified "Confidential". All other persons must be escorted by a guard or a person authorised by the head of an entity of secrets;

3) where the information classified "Secret" or "Top Secret" is stored in the area, a control post must be set up at entrances to the area or to separate premises thereof to identify a person or an identification system must be installed;

4) approaches to buildings must be well lit throughout the night;

5) the premises assigned to the area must be equipped with security, alert and fire alarms;

6) electronic security measures must transmit a double signal warning of an attempt of forced entry into the area or of an unauthorised presence therein not to a single response system;

7) where the information classified "Top Secret" is stored in the area, entry into the area or to the premises located within the area must be monitored by video cameras, and a video archive of 30 calendar days must be kept.

5. Class I security area the premises in which the information classified "Confidential" and above is handled or stored. Entry into the area constitutes direct access to the information stored therein as well as to the

central control of this security area’ s electronic security measures.

6. Class I security area shall be imposed the following requirements:

1) the requirements set in paragraph 4 of this Article;

2) approaches to this security area must be controlled by electronic security measures;

3) the objects brought into and taken out of the area may be checked;

4) this security area shall, by a decision of the head of an entity of secrets or a person authorised by him, be accessed only by the persons holding authorisations to handle or familiarise with the most highly classified information stored in the said security area;

5) no extraneous sources of electromagnetic emissions may be brought into the area;

6) alarms against forced entry, perimeters alarms and fire alarms must be used;

7) the mechanical security measures applied must prevent unauthorised entry into protected premises.

7. Where necessary and in the event of absence of a person entrusted with classified information, repositories of documents, personal safes, metal cabinets may be opened only by the persons authorised by the head of an entity of secrets. Entities of secrets must lay down the procedure for the carrying out and recording of such actions.

8. Where unauthorised persons are suspected to have entered repositories of documents or opened personal safes, metal cabinets, a report shall be immediately forwarded to a responsible person, the head of an entity of secrets and the State Security Department. Until the arrival of officers of the State Security Department, the responsible person and the head of the entity of secrets shall take measures necessary to preserve the place of the incident intact.

Article 32. Functions of a Responsible Person in Implementing the Physical Security of Classified

Information

Article 32. Functions of a Responsible Person in Implementing the Physical Security of Classified Information

A responsible person shall:

1) ensure that appropriate physical security measures are in place and operate properly in the territories and premises where classified information is handled or stored;

2) draft the documents regulating physical security procedures, control the compliance with the procedures laid down and carry out periodic inspections of the physical security arrangements in place;

3) organise training of employees;

4) submit proposals to the head of an entity of secrets or a person authorised by him on the subdivision of premises into security areas;

5) notify the head of an entity of secrets of detected damage to the means of protection and installations of repositories, premises, safes, metal cabinets and take remedial measures.

CHAPTER VII SECURITY OF CLASSIFIED CONTRACTS

CHAPTER VII SECURITY OF CLASSIFIED CONTRACTS

Article 33. Classified Contracts

Article 33. Classified Contracts

1. In performing the functions assigned to them, entities of secrets shall have the right to conclude classified contracts. The procedure for concluding classified contracts shall be laid down by the Government.

2. Prior to signing a contract, the contractor shall obtain a facility security clearance in accordance with the procedure laid down by Article 35 of this Law. The contractor (sub-contractor) and personnel thereof needing, in

the course of execution of the classified contract, to familiarise with classified information must obtain an authorisation to handle or familiarise with classified information prior to signing the contract. The authorisation shall be issued by an entity of secrets which is to award the classified contract. With a consent of the entity of secrets, the contractor shall have the right to employ, for the execution of a part of the classified contract, a sub-contractor which, in accordance with the procedure laid down by Article 35 of this Law, must obtain a facility security clearance.

3. The legal persons participating in the tenders published by foreign states or international organisations on the awarding of a classified contract shall be applied the requirements referred to in Article 35 of this Law, where a foreign state or international organisation requests their security clearances.

4. The undertakings, agencies or organisations operating in foreign states and registered therein may participate in the tenders published by entities of secrets of the Republic of Lithuania on the awarding of a classified contract in the course of execution whereof the Republic of Lithuania information classified “Top Secret”, “Secret” or “Confidential” is going to be released, conditional upon meeting the requirements set for the security of classified contracts by the said states and a relevant conclusion of the foreign state’s responsible institution.

Article 34. Protection of Classified Information in the Course of Execution of a Classified Contract

Article 34. Protection of Classified Information in the Course of Execution of a Classified Contract

1. Upon the conclusion of a classified contract, entities of secrets must control the compliance of the contractor or sub-contractor with requirements for the protection of the classified information released or created in the course of execution of the contract.

2. A classified contract may be unilaterally terminated, where the contractor or sub-contractor does not meet the requirements set for the protection of classified information.

3. Having failed to conclude a contract, upon the execution of a classified contract or having terminated it, the contractor and the sub-contractor must return the entire classified information released to them and hand over the

classified information created in the course of the contract.

Article 35. Issuance of a Facility Security Clearance

Article 35. Issuance of a Facility Security Clearance

1. An institution ensuring the security of classified contracts shall conduct a security inspection of a contractor (sub-contractor), issue a facility security clearance, revoke an issued clearance and control the compliance of contractors or sub-contractors with requirements for the security of classified contracts prior to signing a classified contract and compliance with the requirements in the course of the execution and upon the execution of the classified contract.

2. The aim of a security inspection of an undertaking shall be to determine whether a classified contract may be concluded with a contractor by ensuring an adequate protection of classified information. In the course of the inspection, methods and measures of operational investigative activities may not be used, with the exception of operational investigative interrogation and review of the data entered in operational investigative accounting.

3. Upon the carrying out of the inspection referred to in paragraphs 8-10 of this Article, a facility security clearance shall be issued by the following institutions ensuring the security of classified contracts:

1) where a classified contract is concluded by institutions of the national defence system the Second Investigation Department under the Ministry of National Defence, upon assessing the information submitted by other institutions ensuring the security of classified contracts;

2) where a classified contract is concluded by institutions of the system of the Interior the institutions authorised by the Minister of the Interior, upon assessing the information submitted by other institutions ensuring the security of classified contracts;

3) where a classified contract is concluded by the Special Investigation Service the Special Investigation Service, upon assessing the information submitted by other institutions ensuring the security of classified contracts;

4) where a classified contract is concluded by other entities of secrets the State Security Department, upon assessing the information submitted by other

institutions ensuring the security of classified contracts.

4. Employees of a contractor (sub-contractor) shall be security-cleared by the State Security Department in compliance with the provisions of Articles 16 and 17 of this Law.

5. Entities of secrets shall submit to the institutions ensuring the security of classified contracts:

1) data on the nature, volume of the classified information planned to be released to the contractor or sub-contractor, classifications of the information as well as the services to be provided in the course of execution of a classified contract;

2) a classified contracts security questionnaire as completed by the contractor or sub-contractor and its written consent for inspection;

3) completed questionnaires of the employees of the contractor or sub-contractor applying for authorisations to handle or familiarise with classified information or for security clearances, written consents of the persons for screening and detailed autobiographies.

6. An entity of secrets planning to conclude a classified contract must:

1) appoint the persons responsible for the control of the classified information released in the course of execution of the classified contract and the carrying out of requirements of the classified contract;

2) provide necessary methodological support on the protection of classified information;

3) where necessary, prepare and submit the classification guides required for the execution of the classified contract and specifying the classified information released for the execution of a classified contract or planned to be created, classifications thereof, time periods for classification and conditions of the declassification of this information.

7. The contractor wherewith a classified contract has been concluded as well as the sub-contractor must:

1) in accordance with the procedure laid down by this Law and other legal acts regulating the protection of classified information, organise and carry out the protection of the classified information entrusted or created in the course of execution of the classified contract;

2) ensure that classified information is going to be handled or familiarised with by authorised persons and only in compliance with the need-to-know principle;

3) appoint a person responsible for the execution of the classified contract, organisation, carrying out and control of the protection of classified information;

4) upon the execution of the classified contract or upon the termination of execution thereof prior to the time limit, hand over to an entity of secrets all the documents or products obtained and created in the course of execution of the classified contract containing classified information.

8. Prior to the issuance of a facility security clearance, the following shall be verified:

1) the capital and management structure of the contractor (sub-contractor), origin of the capital, owners and formal registration;

2) administration of the contractor (sub-contractor);

3) financial condition of the contractor (sub-contractor) and committed infringements of laws, the acts of corruption committed by employees or owners of the contractor (sub-contractor);

4) business relations of the contractor (sub-contractor), relations with criminal elements and special services of foreign states activities whereof are hostile to the interests of the State of Lithuania;

5) facilities of ensuring the protection of classified information;

6) security of the employees applying for authorisations to handle or familiarise with classified information or for security clearances.

9. A contractor or sub-contractor must submit to the institutions ensuring the security of classified contracts data on the financial activities of the last financial year as well as other information requested by the institutions ensuring the security of classified contracts.

10. Data on the arrears of a contractor or sub-contractor and committed financial offences shall be supplied to the institutions ensuring the security of classified contracts by tax administrators.

11. The institutions ensuring the security of classified contracts shall have

the right to obtain from state and municipal institutions, banks and other legal persons all required information related to screening of the contractor or sub-contractor and employees thereof for the purpose of issuing a facility security clearance.

12. A facility security clearance shall be valid only in the course of the execution of a specific classified contract. The facility security clearance may be renewed without carrying out of a pre-clearance inspection of an undertaking, conditional upon the lapse of not more than 36 months since the last pre-clearance inspection of the undertaking and where the security of the contractor (sub-contractor) casts no doubt.

13. The authorisations issued to employees of a contractor or sub-contractor to handle or familiarise with classified information shall be valid only in the course of the execution of a specific classified contract, however, not longer than provided for in paragraph 5 of Article 16 of this Law. An authorisation to handle or familiarise with classified information may be renewed without carrying out additional screening of a person, conditional upon the lapse of not more than 36 months since the issuance of the authorisation and where the person’s security casts no doubt.

Article 36. Conditions of Denial of a Facility Security Clearance

Article 36. Conditions of Denial of a Facility Security Clearance

1. A facility security clearance shall not be issued where, in the course of a pre-clearance inspection, it transpires that:

1) a contractor (sub-contractor) is insolvent or does not comply with its contractual obligations to natural or legal persons;

2) the contractor (sub-contractor) has been imposed sanctions for infringements of laws or an enquiry is being conducted in respect thereof, where such violations may result in the threat of a loss or compromise of classified information;

3) the contractor (sub-contractor) is or was engaged in unlawful activities;

4) the contractor (sub-contractor) has submitted false or incorrect data to an institution ensuring the security of classified contracts;

5) the contractor (sub-contractor) does not have facilities to afford protection to the classified information planned to be released or created;

6) the contractor (sub-contractor), through its own fault, has previously been denied a facility security clearance, the facility security clearance has been revoked and reasons for the denial or revocation of the said clearance have not been removed;

7) the employees of the contractor (sub-contractor) to be entrusted with classified information may not, in compliance with paragraph 2 of Article 16 of this Law, be issued an authorisation to handle or familiarise with classified information, and such persons cannot be replaced.

2. A contractor (sub-contractor) shall have the right to appeal against a decision of the institutions ensuring the security of classified contracts not to issue a facility security clearance within 30 working days of the receipt of the said decision to the Commission for Secrets Protection Co-ordination, which shall take a decision binding on an institution ensuring the security of a classified contract.

Article 37. Revocation of a Facility Security Clearance

Article 37. Revocation of a Facility Security Clearance

1. A facility security clearance shall be revoked or a concluded contract shall be terminated, where:

1) through the fault of a contractor or sub-contractor, the classified information entrusted to them has been disclosed or lost;

2) the contractor (sub-contractor) have on repeated occasions violated the requirements set for the protection of classified information or commits grave breaches thereof resulting in the threat of a loss or compromise of classified information;

3) it is established that the contractor (sub-contractor) has concealed data on itself or its activities or has submitted misleading data which have influenced a decision on the issuance of the facility security clearance;

4) at least one circumstance referred to in paragraph 1 of Article 36 arises.

2. A contractor shall have the right to appeal against a decision of the institutions ensuring the security of classified contracts on the revocation of a facility security clearance within 30 working days of the signing of the said decision to the Commission for Secrets Protection Co-ordination, which shall take a decision binding on an institution ensuring the security of a classified contract.

Article 38. Accounting of Facility Security Clearances

Article 38. Accounting of Facility Security Clearances

An institution ensuring the security of classified contracts must, within 10 working days, give written notice to the State Security Department of the facility security clearances issued or revoked. The State Security Department shall keep accounts of the undertakings which have been issued facility security clearances.

Article 39. Functions of Responsible Persons in Concluding and Executing Classified Contracts

Article 39. Functions of Responsible Persons in Concluding and Executing Classified Contracts

1. The responsible person of an entity of secrets shall:

1) submit to the institutions ensuring the security of classified contracts the information referred to in paragraph 5 of Article 35 of this Law;

2) organise the issuance of authorisations to handle or familiarise with classified information to employees of a contractor or sub-contractor and keep accounts of the authorisations issued;

3) organise the release of classified information to a contractor or sub-contractor;

4) control the safeguarding of classified information by a contractor or sub-contractor;

5) by a decision the head of the entity or a person authorised by him, prepare and submit the classification guides required for the execution of a contract;

6) provide methodological support to a contractor or sub-contractor on the protection of classified information.

2. The responsible person of a contractor or sub-contractor shall:

1) submit to the responsible person of an entity of secrets the information referred to in subparagraphs 2 and 3 of paragraph 5 of Article 35 of this Law;

2) ensure the implementation of personnel security procedures;

3) ensure the implementation of requirements for the administration of classified information;

4) ensure the physical security of classified information;

5) ensure the protection of ADP systems and networks.

CHAPTER VIII PROTECTION OF THE AUTOMATED DATA PROCESSING SYSTEMS AND NETWORKS STORING, PROCESSING OR TRANSMITTING CLASSIFIED INFORMATION

CHAPTER VIII PROTECTION OF THE AUTOMATED DATA PROCESSING SYSTEMS AND NETWORKS STORING, PROCESSING OR TRANSMITTING CLASSIFIED INFORMATION

Article 40. Issuance of Authorisations to Process Classified Information via ADP Systems and Networks

Article 40. Issuance of Authorisations to Process Classified Information via ADP Systems and Networks

1. Entities of secrets shall ensure the protection of ADP systems and networks in accordance with the procedure laid down and the requirements set forth by this Law, the Commission for Secrets Protection Co-ordination, the institutions performing the functions of the Security Accreditation Authority,

the National Communications Security Authority and the National Distribution Authority.

2. Entities of secrets must agree design documentation of the ADP systems and networks storing, processing or transmitting the information classified “Top Secret”, “Secret”, “Confidential” with the Security Accreditation Authority or an institution authorised by it, which shall issue an authorisation to use the said networks or systems.

Article 41. Requirements for the Protection of ADP Systems and Networks

Article 41. Requirements for the Protection of ADP Systems and Networks

1. The means of protection used for safeguarding the security of ADP systems and networks must ensure:

1) confidentiality of the classified information stored, processed or transmitted;

2) a possibility to identify users of the systems and networks;

3) integrity of the information stored, processed or transmitted and system services and resources;

4) availability to authorised users of the information stored, processed or transmitted and system services and resources;

5) recording of deliberate or accidental breaches of confidentiality, integrity or availability of the classified information stored, processed or transmitted via ADP systems and networks as well as services and resources of the ADP system and networks;

6) control of interconnection of ADP systems and networks;

7) assessment and verification of adequacy of the protection mechanisms of ADP systems and networks.

2. ADP systems and networks must be equipped with the protection mechanisms and security management procedures preventing breaches of security, detecting occurred breaches of security and restoring the confidentiality, integrity and availability to authorised users of the classified information and services

and resources of the ADP systems and networks as adversely affected by the breaches of security.

3. ADP systems and networks must be equipped with the means of protection allowing to protect the information classified “Confidential” or above against compromise through electromagnetic emissions. The means of protection applied must be commensurate with the risk of the compromise of information and the prejudice likely to be caused upon the disclosure of the information.

4. All operations of the installation and modification of ADP systems and networks must be carried out with the participation and under the supervision of a responsible person. The persons carrying out the maintenance of the communication facilities and computing devices used for storage or transmission of classified information, ADP systems and networks must be cleared to the highest classification level of the information processed, stored or transmitted in the said equipment or system.

5. Installation in the ADP systems and networks processing classified information of the hardware or software not provided for in the ADP systems and networks’ specifications shall be prohibited.

Article 42. Transmission of Classified Information via ADP Systems and Networks

Article 42. Transmission of Classified Information via ADP Systems and Networks

1. When transmitting classified information via ADP systems and networks, the confidentiality, integrity and availability to authorised users of the classified information must be ensured.

2. When transmitting classified information via ADP systems and networks, confidentiality thereof must be ensured by means of the cryptographic methods and products approved by the National Distribution Authority and the telecommunications protection requirements approved by the National Communications Security Authority.

3. Transmission of the information classified “Restricted”, “Confidential”, “Secret” via public telecommunications networks in clear text, with the exception of the cases referred to in paragraph 4 of this Article, shall be prohibited. Transmission of the information classified “Top Secret” via telecommunications networks shall be prohibited.

4. By a decision of the head of an entity of secrets' structural division housing classified information, the information classified "Restricted", "Confidential" and "Secret" may be transmitted in clear text, where a state of war or emergency has been declared and means of encrypting are not available, while speed of delivery is more important than the imminent threat of disclosure of the information.

5. The protection afforded to cryptographic products, mechanisms and classified information must be commensurate with the amount of the prejudice likely to be caused upon a compromise of classified information.

Article 43. Protection of Computer Storage Media

Article 43. Protection of Computer Storage Media

1. All computer storage media used for recording classified information must be adequately identified, held and stored according to the requirements set for the protection of the most highly classified information contained therein.

2. The classified information stored in reusable computer storage media may be deleted and the media declassified only in accordance with the procedures laid down in paragraph 1 of Article 40 of this Law.

Article 44. Functions of a Responsible Person in Organising the Protection of ADP Systems and Networks

Article 44. Functions of a Responsible Person in Organising the Protection of ADP Systems and Networks

A responsible person must:

1) ensure the installation, operation and maintenance of means of protection at the workstations with ADP elements;

2) devise telecommunications plans and schemes and specify therein the location of wires, cables, amount, types, numbering thereof;

3) on the basis of the requirements set by the Security Accreditation Authority, develop, implement and control the procedures for managing security of the ADP systems and networks of an entity of secrets or contractor (sub-contractor) and periodically acquaint therewith administrators and users of the ADP systems and networks;

4) draft the documents on ADP systems and networks required for the obtaining of authorisations to store, process or transmit the information classified "Top Secret", "Secret", "Confidential";

5) ensure that ADP systems and networks are handled by the users authorised to familiarise with the information stored, processed and transmitted in the ADP systems or networks and related to the discharge of their duties as well as control user actions;

6) exercise control of the administration of user passwords and/or of installations for the user identification;

7) organise the administration of classified computer storage media and the physical security of the media;

8) assess the preparedness of a contractor or sub-contractor carry out the requirements set for the protection of the hardware or software housing the information classified "Restricted" and control implementation thereof;

9) organise and check the backup and recovery of the information of ADP systems and networks;

10) verify the information collected about occurrences (process errors, unauthorised users and operation of the system);

11) notify an entity of secrets or a person authorised by him of any gaps in the protection afforded to the ADP systems and networks of the entity of secrets or the contractor (sub-contractor) and the breaches which have occurred and take remedial measures.

CHAPTER IX CONTROL OF THE PROTECTION OF CLASSIFIED INFORMATION

CHAPTER IX CONTROL OF THE PROTECTION OF CLASSIFIED INFORMATION

Article 45. Control of the Protection of Classified Information

Article 45. Control of the Protection of Classified Information

1. Implementation of the policy of protection of the Republic of Lithuania classified information and carrying out of actions of the protection of classified information in all institutions within the country and abroad shall be controlled by the State Security Department. The Department shall:

1) control compliance with the procedure laid down for classifying, using, storing, destroying and declassifying the information classified “Top Secret”, “Secret” and “Confidential”. An entity of secrets must eliminate the deficiencies established in the course of an inspection by the State Security Department within a time limit laid down by the Department and notify thereof the State Security Department;

2) submit proposals to the Government, the Commission for Secrets Protection Co-ordination on the upgrading of the classified information protection system;

3) carries out pre-trial investigation activities in respect of unauthorised holding of classified information, compromise, loss, seizure or other unauthorised acquisition of classified information;

4) provide methodological support to entities of secrets on the protection of classified information.

2. Control of the protection of the information classified “Restricted” shall be exercised by the entities of secrets that have this information at their disposal.

3. The persons exercising control of the protection of classified information must hold authorisations to handle or familiarise with the information classified “Top Secret”. The persons exercising control of the protection of the classified information released to the Republic of Lithuania by other states or international organisations must be appropriately security cleared.

4. The persons exercising control of the protection of classified information shall, in the course of inspections, be familiarised with the contents of classified documents only with a consent of the head of an entity of secrets.

5. The persons exercising control of the protection of classified information

shall have the right:

1) in accordance with the procedure laid down by an entity of secrets, to access the territories and premises where classified information is processed, stored or transmitted;

2) to familiarise with the documents of an entity of secrets regulating the protection of classified information;

3) to carry out inspections of storage of classified documents or copies thereof, where it is required to establish whether a document (copy thereof) has not been lost and is stored in a place specified in accounting documents;

4) to familiarise with physical security measures;

5) to familiarise with ADP systems and networks designed for the processing, storage or transmission of classified information;

6) to request from responsible persons or from the persons handling classified information oral and written explanations about compliance with the procedure for protecting classified information or breaches of this procedure;

7) to engage appropriate specialists, where special knowledge is required at the time of a check.

6. Where classified information is suspected to have been lost or compromised, an enquiry shall be conducted by a decision of the head of an entity of secrets. The inspection must:

1) establish and confirm the classification, contents and volume of the classified information lost or disclosed;

2) establish the persons whose actions could have led to the loss or disclosure of classified information;

3) specify the persons who had this information at their disposal or were familiarised therewith;

4) establish the circumstances of the loss or disclosure of classified information.

7. Where, upon the carrying out of the enquiry provided for in paragraph 6 of this Article and the inspection referred to in Article 27 of this Law, it transpires that classified information has indeed been lost or compromised, the head of an entity of secrets shall immediately notify thereof the State

Security Department, and the officers authorised by it shall carry out a pre-trial investigation.

8. Where, upon the conducting of an enquiry, it transpires that the classified information released to the Republic of Lithuania by foreign states or international organisations has indeed been lost or compromised, notice shall be immediately given to the Commission for Secrets Protection Co-ordination, appropriate services of the state or international organisation which has released the information and the State Security Department, which shall carry out a pre-trial investigation.

CHAPTER X LIABILITY

CHAPTER X LIABILITY

Article 46. Liability for Unauthorised Holding of Classified Information, Compromise, Loss, Seizure or Other Unauthorised Acquisition of Classified Information

Article 46. Liability for Unauthorised Holding of Classified Information, Compromise, Loss, Seizure or Other Unauthorised Acquisition of Classified Information

A person shall be held liable for an unauthorised holding of classified information, the compromise, loss, seizure or other unauthorised acquisition of classified information or for other breaches of the requirements set for the protection of classified information in accordance with the procedure laid down by legal acts.

I promulgate this Law passed by the Seimas of the Republic of Lithuania.

PRESIDENT OF THE REPUBLIC VALDAS ADAMKUS

Annex to
16 December 2003

Republic of Lithuania

Law No. IX-1908

EU LEGAL ACT IMPLEMENTED HEREBY

Council Decision of 19 March 2001 adopting the Council' s security regulations (2001/264/EC).