Act N. 412 of 21 September 2005
on the Protection of Classified Information

Amendment: 119/2007 Coll.
Amendment: 177/2007 Coll.
Amendment: 296/2007 Coll.
Amendment: 32/2008 Coll., of 12 February 2008, effective as from 1 March 2008

The Parliament has passed by resolution the Act of the Czech Republic hereunder:

PART ONE
BASIC PROVISIONS

Section 1
Subject of legislation

This Act shall govern the principles for determination of information as classified information, conditions for access to it and other requirements for its protection, principles for determination of sensitive activities and conditions for their execution and related execution of the state administration.

Section 2
Definition of Terms

For the purpose of this Act, the following definitions shall apply:

a) classified information – information in any form recorded on any medium marked as such in accordance with this Act, whose unauthorised divulgence or misuse could cause damage to the interest of the Czech Republic or could be unfavourable to this interest and that is given on the list of classified information (Section 139);
b) interests of the Czech Republic - preservation of constitutionality, sovereignty and territorial integrity, securing of internal order and security, preservation of international obligations and defence, protection of economy and protection of the life or health of natural persons;

c) breach of the duty to protect classified information - breach of any obligation imposed by this Act or on the basis of this Act;
d) the State body - organizational body of the State according to special legal regulation[1)], region[2)], Capital City of Prague[3)], City District of Capital City of Prague and community[4)] in execution of the state administration in the cases laid down by the special legal regulation; also the Security Intelligence Service[5)], the Military Intelligence[6)] and the Czech National Bank[7)] shall be considered to be the State bodies;
e) responsible person –
   1. minister in the case of a ministry;
   2. competent heads in the cases of other central administrative bodies;
   3. in the case of an organizational State body that was established by another organizational State body the responsible person in the organizational State body carrying out the function of its promoter;
   4. in the case of other organizational State bodies their competent heads;
   5. directors in the case of the Security Intelligence Service and the Military Intelligence;
   6. the Governor in the case of the Czech National Bank;
   7. the director in the case of the Regional Authority;
   8. the director of the Metropolitan Authority of the Capital City of Prague in the case of the Capital City of Prague;
   9. the secretary of the City District Authority in the case of the City District of Capital City of Prague, if there is no such secretary a mayor of the City District;
   10. the secretary of the Metropolitan Authority in the case of a chartered town;
   11. the secretary of the town/community authority in the case of other towns and communities, if there is no such secretary, the town/community mayor;
   12. in the case of the structural component of the territorial self-governing unit the responsible person shall be the responsible person in the case of the territorial self-governing unit carrying out the function of its promoter;
   13. authorised representatives in the case of legal entities not mentioned in points 6-11 above; if more persons act in the name of these other legal entities according to the special legal regulation[8)] who are the authorised representative, or any person who is not the authorised representative, then only the person authorised to act in subject-matters regulated by this Act shall be the responsible person; and
   14. natural persons pursuing business[9)],

f) originator of classified information - the State body, legal entity or natural persons pursuing business that created classified information, or The Office of Industrial Property according to S. 70 par. 4;

g) foreign power – another state or its authority or multinational or international organization or its authority;
h) unauthorised person – natural person or legal entity that does not satisfy conditions for access to classified information laid down herein;
i) briefing – written record that the natural person concerned has been briefed on his/her rights and responsibilities in the area of protection of classified information and on the consequences of their breach;
j) security standard – classified body of rules laying down procedures, technological solutions, security parameters and organizational measures necessary to secure the lowest possible level of protection of classified information;
k) security mode of operation – environment in which the information system operates and which is characterized by the security level of classified information being processed and by the security clearance levels of users.

PART TWO
PROTECTION OF CLASSIFIED INFORMATION

Chapter I
Introductory provisions

Section 3
Damage to the interest of the Czech Republic and Disadvantageousness to the interests of the Czech Republic

(1) Damage to the interest of the Czech Republic, as used in this Act, means the damage to or endangering the interest of the Czech Republic. Depending on the seriousness of the damage caused or seriousness of the threat to the interests of the Czech Republic the detriment shall be graded as extremely serious detriment, serious detriment or simple detriment.

(2) Extremely serious detriment to the interest of the Czech Republic arises in the cases of divulgence of classified information to any unauthorised person or in the case of misuse of classified information, which can result in:

a) imminently endangering sovereignty, territorial integrity or the democratic principles of the Czech Republic;
b) vast losses of human lives or vast threat to life and limb of citizens;
c) extremely serious or long-term damage to the economy of the Czech Republic;
d) significant breach of internal order and security of the Czech Republic;
e) extremely serious endangerment of important security operations or activities of intelligence services;
f) extremely serious endangerment of activities or existence of the North Atlantic Treaty Organisation, European Union or Member State;
g) extremely serious endangerment of the combat capability of the Armed Forces of the Czech Republic, the North Atlantic Treaty Organisation or its Member State or of the Armed Forces of the Member State of the European Union; or
h) extremely serious damage to diplomatic or other relations of the Czech Republic towards the North Atlantic Treaty Organisation, European Union or Member States;

(3) Serious detriment to the interest of the Czech Republic arises in the cases of divulgence of classified information to any unauthorised person or in the case of misuse of classified information, which can result in:

a) endangering sovereignty, territorial integrity or democratic principles of the Czech Republic;
b) significant damage to the Czech Republic in financial, monetary or economic areas;
c) losses of human lives or threat to life and limb of citizens;
d) breach of internal order and security of the Czech Republic;
e) seriously endangering the combat capability of the Armed Forces of the Czech Republic, the North Atlantic Treaty Organisation or its Member State or of the Armed Forces of a Member State of the European Union;
f) seriously endangering important security operations or activities of intelligence services;
g) seriously endangering activities of the North Atlantic Treaty Organisation, European Union or a Member State;
h) seriously breaching diplomatic relations of the Czech Republic towards the North Atlantic Treaty Organisation, European Union, Member States or another state; or
i) serious aggravation of situation causing international tension.

(4) Simple detriment to the interest of the Czech Republic arises as a consequence of the divulgence of classified information to any unauthorised person or misuse of classified information, which can result in:

a) worsening of relations of the Czech Republic with a foreign power;
b) endangering the security of an individual;
c) endangering the combat capability of the Armed Forces of the Czech Republic, the North Atlantic Treaty Organisation or its Member State or of the Armed Forces of a Member State of the European Union;
d) endangering security operations or activities of intelligence services;
e) endangering activities or the existence of the European Union or any of its Member States;
f) obstructing, impeding or endangering the vetting or investigation of specially grave offences or the facilitation of their commission;
g) occurrence of damage not insignificant to the Czech Republic; or
h) serious infringement of economic interests of the Czech Republic.

(5) Disadvantageous to the interests of the Czech Republic is the divulgence of classified information to any unauthorised person or misuse of classified information, which can result in:

a) a breach of activities of the Armed Forces of the Czech Republic, the North Atlantic Treaty Organisation or its Member State or of the Member State of the European Union;
b) obstructing, impeding or endangering the vetting or investigation of offences other than that outlined in the paragraph 4 (f) above or the facilitation of their commission;
c) damage to important economic interests of the Czech Republic or to economic interests of the European Union or its Member State;
d) a breach of important commercial or political negotiations of the Czech Republic with a foreign power; or
e) a breach of security or intelligence operations.

Section 4
Security classification levels

Classified information shall be classified as follows

a) TOP SECRET in cases where unauthorised divulgence of information to an unauthorised person or its misuse can result in extremely serious detriment to the interests of the Czech Republic;
b) SECRET in cases where unauthorised divulgence of information to an unauthorised person or its misuse can result in serious detriment to the interests of the Czech Republic;
c) CONFIDENTIAL in cases where unauthorised divulgence of information to an unauthorised person or its misuse can result in simple detriment to the interests of the Czech Republic;
d) RESTRICTED in cases where unauthorised divulgence of information to an unauthorised person or its misuse can be disadvantageous to the interests of the Czech Republic.

Section 5
Forms of securing of the protection of classified information

The protection of classified information shall be based on

a) personnel security, which consists of selection of natural persons who should have access to classified information, verification of conditions for their access to classified information, their training and protection;
b) industrial security, which is the application of measures to ascertain and verify conditions for access by the facility to classified information and to secure handling of classified information by the facility in accordance with this Act;
c) administrative security, which is the system of measures for originating, receiving, recording, handling, sending, transportation, transmission, hand carriage, storing, discarding, archiving, or another method of handling of classified information, as the case may be;
d) physical security, which is the system of measures designed to prevent or impede unauthorised access to classified information, or to provide evidence of any access or of any attempted access;
e) information and communication systems security, which is the system of measures to provide confidentiality, integrity and availability of classified information handled by these systems, and liability of the administration and user for their implementation in information or communication systems; and
f) cryptographic protection, which is the system of measures for the protection of classified information using cryptographic methods and cryptographic material in processing, transmission or storing of classified information.

Chapter II
Personnel security

Conditions for access of natural persons to RESTRICTED classified information
Section 6

(1) A natural person may be granted access to RESTRICTED classified information who requires access to this information in order to perform his/her official tasks or services (on a need-to-know basis), who is a holder of the Notice of compliance with conditions for access to RESTRICTED classified information (hereinafter "the Notice"), the Personnel Security Clearance (S. 54) or the Certificate (S. 80) and has been briefed, save as otherwise provided for in this Act or in the special legal regulation (S. 58-62).

(2) The Notice will be issued to the natural person who:

a) has full legal capacity;
b) is aged 18 or over;
c) has no criminal record.

(3) Fulfilment of the conditions outlined in paragraph 2 above shall be verified and the Notice to the natural person shall be issued by the person who is responsible in respect of this natural person in a framework of the service relationship or employment relationship, member relationship or similar relationship or by a person delegated by this responsible person. If there is no such a responsible person according to the first sentence, the compliance with conditions outlined in paragraph 2 will be verified and the Notice to the natural person will be issued on the written request by the National Security Authority (hereinafter "the Authority").

Section 7

(1) The statement made by the natural person of the legal capacity will prove the condition of legal capacity. The condition of age will be proved by identification card or by travel documents of the natural person. The condition of his/her suitability will be proved by a statement of no criminal records[11)] and, in the case of a foreigner, by similar document issued by the person's country of citizenship, as well as by the document of the country in which the person has resided for at least six consecutive months. Document certifying no criminal records shall apply only for three months from the date of its issuance.

(2) The natural person shall submit documents according to paragraph 1 above.

(3) The form of statement of the legal capacity of the natural person will be provided for by the implementing regulation.

Section 8
Condition of no criminal records

The condition of no criminal records will be satisfied by the natural person who has not been finally and conclusively condemned of an intentional crime or of a crime relating to the protection of classified information, or by the natural person who is accounted to be a person who had not been condemned.

Section 9

(1) Before the initial access to classified information at the RESTRICTED level, the briefing of the natural person shall be arranged by the person who is responsible in respect of this natural person in a framework of the service relationship or employment relationship, member relationship or similar relationship. If there is no such a responsible person according to the first sentence, the briefing shall be arranged by the responsible person of the authority that will grant access to classified information. The briefing shall be acknowledged by the natural person concerned and by an individual, who conducted the briefing; one copy will be forwarded to the briefed person and one copy will be filed[12)].

(2) The issuing authority of the Notice shall verify every three years from the date of its issuance fulfilment of conditions laid down in S. 6 par. 2(a) and 2(c); fulfilment of these conditions may be verified by the authority even before the expiration of the stated period if reasonable doubts are present indicating that the person concerned no longer fulfils any of these conditions.

(3) Validity of the Notice expires or will be terminated

a) by serving a written notification of the issuing authority of the Notice that the natural person no longer fulfils condition outlined in S. 6 par. 2(a) or 2(c);
b) by the end of the service relationship or employment relationship, member relationship or similar relationship within the framework of

which the natural person had access to classified information;

c) by commencement of service relationship or employment relationship, member relationship or similar relationship within the framework of which the natural person should have access to classified information if the Notice has been issued by the Authority in accordance with S. 6 par. 3;
d) upon death or upon declaration of the death of a person concerned;
e) as a result of theft or loss;
f) as a result of damage to such an extent that its entries become illegible or its integrity is damaged; or
g) by serving a written notification of the issuing authority of the Notice that the natural person did not fulfil conditions according to S. 10 par. 2(b) within a prescribed period.

(4) When the validity of the Notice ends according to par. 3(a) and (g), the issuing authority of the Notice shall prevent the natural person concerned from having access to classified information and shall notify in writing this natural person thereof. The reasons of termination of the validity of the Notice shall be given in this written notification. The issuing authority of the Notice shall make the written record of the validity termination if the validity of the Notice ends according to par 3 (b), (c), (d) or (f), which shall be filed by the issuing authority[12)].

(5) Access of the natural person to classified information is not affected by termination of the validity of the Notice according to par. 3 (e) and (f); in this case the issuing authority of the Notice shall grant, on written request, a new Notice within five days of the service thereof, which substitutes the original Notice.

(6) When the validity of the Notice ends according to par. 3 (a) the natural person shall forward the Notice within five days of the service of the written notification thereof, and in the case of termination according to par. 3 (b) or (c), within five days of this termination to the issuing authority of the Notice.

(7) In the case of termination of the validity of the Notice it shall be assumed that the natural person has not been briefed.

(8) The forms of the Notice and the briefing will be determined by the implementing legal regulation.

Section 10

(1) Conditions outlined in S. 6 par 2(a) and (c) must be fulfilled by the natural person, who is a holder of the Notice, throughout the period of access to RESTRICTED classified information.

(2) The natural person according to the paragraph 1 shall

a) notify in writing the issuing authority of the Notice of all changes concerning conditions outlined in S. 6 par. 2(a) and (c), as well as of all changes to data set out in the Notice, within five days of the date when a change occurred;
b) submit within a prescribed period, in cases according to S. 9 par. 2, at the request of the issuing authority of the Notice, a statement of criminal records[11)] and a statement of the legal capacity; the validity of these documents shall not extend beyond three months;

Conditions for access of a natural person to classified information classified TOP SECRET, SECRET or CONFIDENTIAL

Section 11

(1) Only such natural person may be granted access to TOP SECRET, SECRET or CONFIDENTIAL classified information whose duties, work, functions or services necessarily require such access, who is a holder of a valid PSC (S. 54) of the appropriate security level and has been briefed, save as otherwise provided for in this Act or in the special legal regulation (S. 58-62).

(2) Before the initial access to classified information at the levels TOP SECRET, SECRET, CONFIDENTIAL the briefing of the natural person shall be arranged by the person who is responsible in respect of this natural person in a framework of the service relationship or employment relationship, member relationship or similar relationship. If there is no such a responsible person according to the first sentence, the briefing shall be arranged by the responsible person of the authority that may grant access to classified information. The briefing shall be acknowledged by the natural person concerned and by an individual who conducted the briefing, one copy will be forwarded to the briefed person and one copy will be filed[12] and one copy will be sent to the Authority. The duty to send one copy of the briefing does not apply to the Intelligence Services of the

Czech Republic[13)] (hereinafter "the Intelligence Services") in the cases according to S. 140 par. 1 (a), and to the Ministry of the Interior in the cases according to S. 141 par. 1.

(3) The Prime Minister will carry out the briefing of the Director of the Authority and of the Director of the Intelligence Service; paragraph 2 shall apply similarly concerning acknowledgement, sending and filing of the copy of the briefing.

(4) In the case of termination of the validity of the PSC (S. 56 par. 1) it shall be assumed that the natural person has not been briefed.

Section 12
Conditions for issuance of the Personnel Security Clearance

(1) Personnel Security Clearance (hereinafter "the PSC") will be issued to the natural person by the Authority, who

a) is a national of the Czech Republic or a national of any Member State of the European Union or of the North Atlantic Treaty Organization;
b) meets the conditions outlined in S. 6 par. 2;
c) is personally eligible;
d) is security reliable.

(2) Conditions outlined in paragraph 1 shall be met by the natural person throughout the period of validity of the PSC (S. 55)

Section 13
Personal eligibility

(1) The natural person who does not suffer from any disorder or problem that could affect his/her reliability or ability to maintain confidentiality of information will fulfill the condition of the personal eligibility.

(2) Personal eligibility according to paragraph 1 will be verified on the basis of the statement of personnel eligibility and in the cases determined by this Act (S. 106) also on the basis of expert reports on the personal eligibility.

(3) The Intelligence Service will verify the personal eligibility of its members, employees and job or service candidates in cases according to S. 140 par. 1 (a), and the Ministry of the Interior in cases according to S. 141 par. 1, on the basis of a statement concerning personal eligibility or on the basis of psychological examination by psychological centre of the Intelligence Service or of the Ministry of the Interior; for purposes of the application according to S. 94 for the security classification level TOP SECRET, the personal eligibility shall be verified on the basis of psychological examination.

Section 14
Security reliability

(1) The natural person who has not been ascertained to be a security risk will fulfill the condition of personal reliability.

(2) The following shall be considered to be a security risk

a) serious or repeated activities against interests of the Czech Republic; or
b) activities consisting of suppressing human rights or liberties, or support of such activities.

(3) Also the following may be considered to be a security risk

a) assignment to the intelligence or counterintelligence unit of the former State Security, to the Intelligence Department of the General Staff of the Czechoslovak People's Army or to the Internal Protection Department of the Correctional Treatment Facility, or provable co-operation with the former State Security or with the Intelligence Department of the General Staff of the Czechoslovak People's Army or with the Internal Protection Department of the Correctional Treatment Facility;
b) use of another identity;
c) intentional breach of legal regulations that can result in damage to interests of the Czech Republic;
d) conduct and lifestyle that may render the individual liable to influence, and may affect his or her trustworthiness or ability to maintain confidentiality of information;
e) contacts with a person who has been or is engaged in activities aimed against interests of the Czech Republic;
f) sentence imposed upon a final and conclusive judgment;
g) deliberately providing false or misleading information or deliberate omission of material information for unbiased determination of facts of the case during the procedure according to Part four of this Act, or not reporting changes to data listed in the annex to this PSC application (S. 94) or in any other material provided to the Authority in annex to this application;

h) breach of duties in protection of classified information; or
i) evidence of unexplained financial or property affluence with respect to duly declared income of the natural person.

(4) In the case of an application according to S. 94, security risks outlined in paragraphs 2 and 3 (a) will be investigated for a period from the applicant´s fifteenth birthday to the present; investigation of security risks outlined in paragraphs 3 (b) to (j) shall cover the last 10 years from the date of submitting the application for the security level CONFIDENTIAL, 15 years for the security level SECRET and 20 years for the security level TOP SECRET, or the period shall be covered from the applicant´s fifteenth birthday to the present, whichever is shorter.

(5) The security risk outlined in paragraph 3 (b) shall not be considered to be a security risk if the natural person used another identity for legal reasons.

(6) The following factors shall be considered in evaluation of whether the fact outlined in paragraph 3 constitutes the security risk – the extent to which it can affect capability to maintain confidentiality of information, whether the event was or was not recent, its extent, the character and conduct of the natural person over a period specified in paragraph 4.

(7) In evaluation of security risks according to paragraph 3 the Intelligence Service can carry out physiodetection examinations of its members, employees and job or service candidates, if ascertained facts give rise to doubts as to the ability of the natural person to maintain confidentiality of information.

Chapter III
Industrial security

Conditions for access of the facility to classified information and forms of access of the facility to classified information
Section 15

The facility may be granted access to classified information, which shall have access to information in order to perform official tasks or services and is a holder of valid facility security clearance (S. 54) for appropriate security classification level, save as otherwise provided for in this Act (S. 58 to 62).

Section 16
Conditions for issuance of the Facility Security Clearance

(1) Facility Security Clearance (hereinafter "the FSC") will be issued by the Authority to the facility

a) which is economically stable;
b) which is reliable in terms of security;
c) which is able to secure the protection of classified information; and
d) if the responsible person and proctors are holders of valid PSC at least for such a security classification level for which the facility applies in application for granting FSC, or if the responsible person and proctors are holders of the valid Notice in the case when the FSC for the security classification level RESTRICTED is to be issued.

(2) Conditions outlined in paragraph 1 shall be fulfilled by the facility until expiration of the FSC (S. 55).

Section 17
Economic stability

(1) The condition of economic stability will not be fulfilled by the facility

a) the existence of which was terminated[14)];
b) on which the moratorium has been placed upon the court order[15)];
c) in respect of property of which the adjudication of bankruptcy has been issued[15)];
d) in the case of which compulsory administration was established.

(2) The condition of economic stability will also not be fulfilled by the facility

a) which is deficient in the social welfare insurance payment, in state employment policy allowance or public health insurance payments, including late payment fees;
b) which is deficient in payment of the income tax, value added tax or other tax arrears, including late payment fees, or assessed customs duty, including interests, if any;
c) which permanently or repeatedly does not fulfil financial duties towards the State, natural or legal persons; or
d) in the case where the decision was made to distrain property.

Section 18
Security reliability

(1) The condition of security reliability will not be fulfilled by the facility, which was determined to be a security risk.

(2) A security risk shall be considered to be any activity of an authorised representative or of a member of the authorised representative, of a member of the control body or of a proctor against interests of the Czech Republic.

(3) Also the following may be considered to be a security risk

a) deliberately providing false information or omission of material information necessary for objective and full determination of facts of the case during the procedure of verifying conditions for issuance of the FSC, or omission to report changes to data listed in the application according to S. 96 or in other material provided to the Authority with respect to this application;
b) capital, financial or commercial relations with other natural or legal persons or with a foreign power engaged in activities aimed against interests of the Czech Republic;
c) personal instability of the authorised representative or of the control body or with respect to persons of proctors;
d) if the facility is the joint-stock company with another form of shares than registered shares;
e) if a company with another form of shares than registered shares is a partner with controlling influence on selection or the designation of an authorised representative or of the control body of the facility;
f) breach of obligations in protection of classified information;
g) final and valid conviction of an intentional offence of the natural person who is a partner of the facility;
h) intentional breach of legal regulations by individuals authorised to act on behalf of or for the facility that could cause damage to interests of the Czech Republic; or
i) relations of foreign nationals employed by the facility with natural or legal persons or with a foreign power that has been or is engaged in activities aimed against interests of the Czech Republic.

Section 19
Eligibility to secure the protection of classified information

The condition of eligibility to provide for the security protection of classified information will not be fulfilled by the facility, which is not able to ensure that respective forms of the protection of classified information according to this Act will be established and complied with taking into account the corresponding security classification level and the form of display of classified information.

Section 20
Form of access of the facility to classified information

(1) The facility may have access to classified information that

a) is originated by or released to the facility; or
b) is not originated by or released to the facility, but which is accessible by persons acting on behalf of or for the facility, in connection with performance of work or other activities for the facility on the basis of the contract.

(2) In the case of access according to paragraph 1 (b) the facility shall fulfil the condition according to the S. 16 par. 1 (c) only by ensuring the protection of classified information based on the personnel security [S. 5 (a)].

Chapter IV
Administrative Security

Markings and accounting of classified information
Section 21

(1) The information that complies with elements according to S. 4 and that is included in the list of classified information shall be marked by the originator with the name of the originator, security classification level of the information, its registration mark, the date of its creation, unless otherwise provided herein.

(2) Classified information provided to the Czech Republic by a foreign power shall be marked with the security classification level in accordance with S. 4, by the State body, legal person or natural person pursuing business, if they are first to register this classified information (S. 77 to 79), in accordance with international agreement by which the Czech Republic is bound and under authority of which

classified information is released, including relevant abbreviations according to this agreement (for example "EU", "EURA" or "NATO"), or as prescribed by a foreign power or in accordance with the security classification level marked on the released classified information by a foreign power; the name of the originator and the date of creation of classified information will not be marked.

(3) Also the respective additional marking (special category designator) shall be applied to a special category information signifying that the information shall be protected in accordance with more stringent conditions (hereinafter "the Special Handling Regime") in the areas determined in particular by an international agreement to which the Czech Republic is bound, or determined by regulations of an international organization of which the Czech Republic is a member (for example the marking "CRYPTO" in the case of information from the area of cryptographic protection, and the marking "ATOMAL" in the case of information from the area of weapons of mass destruction).

(4) If the marking according to par. 1 to 3 cannot be made on the information, it shall take such a form so that it is possible to determine the necessary details at any moment.

(5) Classified information shall be registered in administrative aids specified by the implementing legal regulation; this requirement will not apply to RESTRICTED source materials on information classified RESTRICTED if the responsible person takes the decision not to register them. Also transmission, receiving or any other movement of classified information shall be registered in administrative aids.

(6) Reproductions, copies or translations of classified information classified TOP SECRET or extract of this information may be produced only with the written consent of the originator; in the case of information classified SECRET or CONFIDENTIAL they may be produced only with the written consent of immediate superior officer.

(7) Classified information may be transported or carried only in portable containers or in closed package depending on its security classification level and on its carrier; it can be transmitted only by courier service or by postal services licence holders[17)].

(8) The recipient shall acknowledge receipt of classified information, unless otherwise provided herein (S. 23 par. 1).

(9) In the course of a destruction period prescribed according to the special legal regulation[18)], classified information may be lent only to such natural persons who are, with respect to the State body, to the legal person or natural person pursuing business, in a service relationship or employment relationship, a member relationship or a similar relationship.

(10) Discarding procedure of classified information shall be in accordance with the special legal regulation[18)].

Section 22

(1) The security classification level shall be marked on classified information at the time of its creation, unless otherwise provided herein (S. 70).

(2) Qualifying markings of classified information shall be maintained throughout the duration of reasons for confidentiality. The security classification level shall not be changed or declassified without the consent of the originator or releasing foreign power.

(3) If necessitated with respect to the nature of classified information, the originator shall indicate on classified information the period for which it shall be kept secret; the security classification level will expire on an indicated date.

(4) The security classification level shall be immediately changed or information shall be declassified by the originator, when it has been verified that reasons for classification of information cease to exist, that reasons for classification do not correspond to the set security classification level or if the classification level has been determined without authorization, and this declassification or new classification level shall be indicated by the originator on the corresponding classified information.

(5) The originator shall ensure that information originated is reviewed no less frequently than every five years from the date of its creation to ascertain whether the reason for its classification still applies.

(6) If the originator changed or declassified the security classification level according to paragraph 4,

he shall inform immediately in writing all addresses of this classified information. Addressees of classified information shall inform immediately in writing all other addressees authorised by them to have access to this classified information.

(7) The addressee shall indicate declassification or change in the classification level of classified information after notification of the change or declassification according to paragraph 6.

(8) In the case of termination of the existence or dissolution of the originator the declassification or change in the security classification according to paragraph 4 and notification according to paragraph 6 will be performed by its legal successor, in the absence of the legal successor or if the legal successor does not comply with conditions regulating access to classified information, the Authority will assume this responsibility.

Section 23

(1) With the exception of classified information requiring the Special Handling Regime, the duty outlined in S. 21 par. 8 will not apply to the transmission of information:

a) classified up to SECRET between the Intelligence Services and similar services of a foreign power, conducted within the frame of co-operation according to the special legal regulation[19)] when the procedure according to S. 21 par. 8 cannot be complied with;
b) classified RESTRICTED if so determined by the responsible person and a foreign power or the originator of classified information will not specifically require any receipt.

(2) The implementing legal regulation shall determine

a) the method of marking elements on classified information according to S. 21 par. 1 to 4, and S. 22 par. 1, 3, 4 and 7, particularly in connection with the security classification level of classified information and in connection with the carrier of classified information;
b) the types of administrative aids outlined in S. 21 par. 5, particularly in the form of books, workbooks or sheets, their elements and organizational and technical requirements for their maintaining and the volume of RESTRICTED source materials on information classified RESTRICTED;
c) the elements of the consent to make reproductions, copies, extracts and translations of classified information (S. 21 par. 6), the method of necessary marking and the method of making extracts;
d) details concerning transport, transmission, carrying, reception and lending of classified information according to S. 21 par. 7 to 9 and details concerning the subsequent related handling of classified information, including organizational securing of these activities, requirements for portable containers and packages and marking relevant elements on them, particularly in connection with the security classification level of classified information and in connection with the carrier of classified information.

(3) Provisions of this Chapter do not relate to processing and transmission of classified information in information systems and cryptographic equipment.

(4) The Authority promulgates by notification in the Collection of Laws of the Czech Republic conversion tables of security classification levels according to international agreements to which the Czech Republic is bound.

Chapter V
Physical security

Section 24

(1) Premises, security areas and areas designated as the meeting rooms will be determined for the purposes of ensuring the protection of classified information within the frame of physical security.

(2) Premises will be a building or another limited location housing the security area or areas designated as the meeting rooms.

(3) The security area will be a limited location within the boundary of the premises.

(4) The area designated as the meeting room will be a location within the boundary of the premises. Classified information at the classification level TOP SECRET or SECRET may be normally discussed only within areas designated as the meeting room.

(5) Classified information shall be handled

a) in security areas;

b) within premises outside the confines of the security area if it is ensured that unauthorised individuals are denied access to classified information; or
c) in justified cases and with the written consent of the responsible person or security officer, outside confines of premises if it is ensured that unauthorised individuals are denied access to classified information.

(6) Classified information shall be stored in the security area and within this area in the security container, lockable cabinet or in other security container, if necessary, subject to conditions set out by the implementing legal regulation.

Section 25

(1) According to the highest level of classification of classified information involved, security areas will be graded as follows

a) TOP SECRET;
b) SECRET;
c) CONFIDENTIAL; or
d) RESTRICTED.

(2) According to the possibility to have access to classified information security areas will be organised and structured so as to correspond to one of the following classes

a) Class I, an area in which an entry into the area constitutes, for all practical purposes, access to classified information;
b) Class II, an area in which an entry into the area does not constitute access to classified information.

(3) All entry and exit into and from the security area shall be controlled by measures according to S. 27. Unauthorised person may have entry only to security area Class II if accompanied at all times by the person who is authorised entry to this area.

Section 26
Discussions involving classified information

(1) The responsible person shall ensure that in the area designated as the meeting room according to S. 24 par. 4, classified information to be involved is not threatened or no leakage of this classified information is possible.

(2) In order to meet the requirements according to paragraph 1 the responsible person shall request the Authority to carry out the technical security examination for an unauthorised use of technical devices intended for obtaining data within the perimeter of the area designated as the meeting room. This examination shall be provided by the Authority in co-operation with Intelligence Services and the Police of the Czech Republic (hereinafter "the Police"). For their own needs the Intelligence Services and the Police carry out the examination independently.

(3) All entry and exit into and from the area designated as the meeting room shall be controlled by measures according to S. 27. An unauthorised person may have access to the area designated as the meeting room only if accompanied by the person who is authorised to access to this area.

Section 27

Measures of the physical security are as follows

a) guards;
b) special handling arrangements;
c) technical means.

Section 28

(1) Full-time protection by guard shall be ensured at premises housing the security area of the category

a) TOP SECRET, at least two persons at the premises;
b) SECRET, at least one person at the building and one another person who shall be able to take action on the basis of combination of measures according to S. 30 par. 1(b), (c) and (f) enabling response within a reasonable timescale in the event of a breach of protection regime of classified information;
c) CONFIDENTIAL, at least one person who shall be able to take action on the basis of combination of measures according to S. 30 par. 1(b) and (c) enabling response within a reasonable timescale in the event of a breach of protection regime of classified information.

(2) In the case of premises housing the security area classified not higher than RESTRICTED the guards will be provided as determined by the responsible person.

(3) In the case of premises housing the area designated as the meeting room where classified information at the level TOP SECRET are regularly

discussed, at least two guards shall be provided at the premises. In the case of premises housing the area designated as the meeting room where classified information at the level SECRET are regularly discussed, the guards shall be provided at least by one person at the premises and by one another person who shall be able to take action on the basis of a combination of measures according to S. 30 par. 1(b), (c), (d) and (f) enabling response within a reasonable timescale in the event of a breach of protection regime of classified information.

(4) Guards shall be provided by employees of the State body, of the legal person or by employees of the natural person pursuing business in the corresponding premises, by members of armed forces or armed corps or by members of armed forces of a foreign power or by employees of the Security protection service.

Section 29

Authorization of persons and vehicles to enter and exit the area, authorization of persons to enter the security area and the area designated as the meeting room and the method of control of these authorizations, as well as the manipulation of keys and identification means used for the entry control systems according to S. 30 par. 1 (b), and the method of handling of technical means and their use shall be determined by special handling arrangements. The special handling arrangements shall also determine authorizations for exit of individuals and vehicles from the premises and for their control, as well as conditions and methods of control of movement of persons within the perimeter of premises, security area and area designated as the meeting room, and the method of control and remove of classified information from the premises, from the security area and from the area designated as the meeting room.

Section 30

(1) The technical means shall be in particular

a) mechanical barriers;
b) electrical locking mechanisms and entry control systems;
c) electrical alarm annunciation equipment;
d) closed circuit television systems;
e) emergency systems;
f) electrical fire detection devices;
g) devices for physical searches for dangerous substances or objects;
h) devices for physical destruction of data carriers;
i) devices against passive and active eavesdropping of classified information.

(2) Marks score (S. 31 par. 1) will be assigned to certified technical means [S. 46 par. 1 (a)] and to uncertified technical means approved by the responsible person.

(3) In the case of engagement of the Czech Republic in international armed conflict, international rescue or humanitarian action, in other international missions, in cases of declaration of belligerency, state of endangering the community, emergency or endangering of the State[20)], as well as during activities of the Armed Forces of the Czech Republic within the frame of exercises and military operational training using military systems and equipment outside the places of permanent deployment of the army unit, the technical means listed in paragraph 1 may be replaced by augmented security guards at a higher level than that outlined in S. 28, which will be carried out by the armed forces staff or by armed corps staff on the basis of the special legal regulations[21)] or by the armed forces staff of a foreign power.

Section 31

(1) The level of safeguarding of the area designated as the meeting room and of the security area by the physical security measures shall be determined by marks score of these measures depending on the risks assessment; marks score and the lowest level of safeguarding shall be determined by the implementing legal regulation.

(2) The measures of the physical security or combination of more of these measures must correspond at least to the lowest levels of safeguarding of the area designated as the meeting room or of the security area, and these measures shall be determined depending on the risks assessment and on the security level of classified information that is regularly discussed in the meeting area or on the category of the security area.

(3) The responsible person will set measures according to paragraph 2 in the physical security project.

(4) Assessment of risks must be made continuously and the level of physical security measures shall be adjusted, as necessary.

(5) The State body, legal person or natural person pursuing business shall ensure and verify regularly whether physical security measures being

used correspond with the physical security project and with legal regulations in the area of protection of classified information.

Section 32
Physical security project

(1) In the case of premises housing security areas classified at levels TOP SECRET, SECRET or CONFIDENTIAL the following shall be contained in the physical security project

a) indication of premises and security areas including their perimeters and indication of categories and classes of security areas;
b) risks assessment;
c) method of application of physical security measures;
d) operating rules of the premises;
e) emergency plan of safeguarding of premises and security areas.

(2) In the case of premises housing only security areas classified at the level RESTRICTED the following shall be contained in the physical security project

a) indication of premises and security areas including their perimeters and indication of categories and classes of security areas;
b) method of application of physical security measures.

(3) In the case of premises housing the area designated as the meeting room the following shall be contained in the physical security project

a) indication of premises and indication of the area designated as the meeting room, including their perimeters;
b) risks assessment;
c) method of application of physical security measures;
d) operating rules of premises;
e) emergency plan of safeguarding of premises and area designated as the meeting room.

(4) The physical security project shall be deposited with the responsible person or with the security officer.

Section 33
Delegating provisions

The implementing legal regulation shall determine

a) the method of storing classified information depending on the level of its security classification (s. 24 par. 6);
b) the organizational requirements for fulfilling the duties of security guards (S. 28) and for safeguarding of the area designated as the meeting room or for safeguarding of the security area by these guards, including determination of the category of individuals listed in S. 28 par. 4 depending on the security classification level of classified information that is regularly discussed in the area designated as the meeting room, or on the category of the security area;
c) the details of special handling arrangements (S. 29);
d) the requirements for technical means listed in S. 30 par. 1 and for safeguarding of the area designated as the meeting room or for safeguarding of the security area by this means depending on the security classification level of classified information that is regularly discussed in the area designated as the meeting room, or on the category of the security area;
e) the marks score of individual physical security measures and marks score of the lowest level of safeguarding of the area designated as the meeting room or marks score of the lowest level of safeguarding of the security area, including the basic method of the risks assessment (S. 31 par. 1 and 2);
f) the frequency and the method of records of verification whether the physical security measures used conform with the physical security project and with legal regulations in the area of protection of classified information, depending on the security classification level of classified information (S. 31 par. 5);
g) the content of operating guidelines of premises and content of the emergency plan for safeguarding premises, security areas and areas designated as the meeting rooms (S. 32 par. 1 (d) and (e) and S. 32 par. 3 (d) and (e)].

Chapter VI
Information and communication systems security

Section 34
Information system

(1) For the purpose of this Act the information system handling classified information will consist of one or more computers, their software, connected peripherals, administration of this information system, together with associated processes or devices able to collect, create, process, store, display or transmit classified information (hereinafter "the Information System").

(2) The Information Systems must be certified by the Authority [S. 46 par 1(b)] and approved for operation in writing by the responsible person.

(3) Classified information may be handled only in the Information System that fulfils conditions according to paragraph 2.

(4) The responsible person must notify approval for operation of the Information System according to paragraph 2 to the Authority in writing within 30 days of this approval.

(5) The implementing legal regulation shall determine

a) requirements for the Information System and conditions of its secure operating depending on the security classification level of classified information handled by the system and on the security operation mode; and
b) content of the Information System security documentation.

Section 35
Communication system

(1) For the purpose of this Act the communication system handling classified information (hereinafter "the Communication System") shall be a system ensuring the transmission of this information between end-users, and involving communication terminals, transmission environment, cryptographic means, operators and operational conditions and procedures.

(2) The Communication System shall not be operated without the project of Communication System security approved by the Authority. The approval of the project of the Communication System security shall be required in writing from the Authority by the State body, legal person or natural person pursuing business who will operate it.

(3) Classified information may be handled only in the Communication System that meets conditions according to paragraph 2.

(4) The project of the Communication System security shall contain

a) Communication System security policy;
b) organizational and operational procedures of operating of the Communication System;
c) operating regulations on the security administration of the Communication System;
d) operating regulations of the Communication System user.

(5) The implementing legal regulation shall stipulate

a) the content of the application for approval of the project of Communication System security; and
b) the elements of the project of Communication System security and methods of and conditions for its approval.

Chapter VII
Protection of classified information in copying machines, display devices or memory typewriters

Section 36

(1) The protection of classified information must be secured during its electronic processing in copying machines, display devices or memory typewriters that are not parts of information or Communication Systems.

(2) In the cases under paragraph 1 the State body, legal persons and natural persons pursuing business shall prepare security operation guidelines of copying machines, display devices or memory typewriters.

(3) Classified information may be processed in devices falling under paragraph 1 only in accordance with their security operation guidelines.

(4) The following shall be stated in the security operation guidelines according to paragraph 2

a) the method of operating of copying machines, display devices or memory typewriters; and
b) operation guidelines of the user of copying machines, display devices or memory typewriters.

(5) Implementing legal regulation shall determine conditions of secure operation of copying machines, display devices or memory typewriters depending on the security classification level of classified information.

Chapter VIII
Cryptographic protection

Section 37

(1) Cryptographic material means the cryptographic equipment, key material or cryptographic document.

(2) The cryptographic equipment means classified technical device or software product used for the purposes of cryptographic protection, or device or equipment used for the production or testing of the key material. Cryptographic equipment must be certified by the Authority [S. 46 par. 1(c)].

(3) Key material means the cryptographic key on the corresponding carrier. Cryptographic key means the classified variable parameter necessary for unique encryption, deciphering or authentication of data.

(4) Cryptographic document means an instrument or data carrying media containing classified information concerning cryptographic protection.

(5) A cryptographic site means a site for production or testing of key material, storing cryptographic material or for distribution and recording of cryptographic material. The cryptographic site must comply with security standards and shall be subject to approval by the responsible person prior to live activation.

(6) The cryptographic site, which is determined for production or testing of key material or which is distribution and accounting centre of cryptographic material of the State body, legal persons or natural persons pursuing business must be certified by the Authority prior approval to live activation by the responsible person [S. 46 par. 1(d)].

(7) A State body, legal person or natural person pursuing business that carry out cryptographic protection shall keep records of cryptographic material, cryptographic protection staffs, operators of cryptographic equipment and couriers of cryptographic material.

(8) Records according to paragraph 7 shall be kept in administrative aids of the cryptographic protection.

(9) Administrative aids of the cryptographic protection means aids for recording, transmission, receiving and other methods of accounting of movement of cryptographic material, as well as aids for accounting of cryptographic protection staffs, operators of the cryptographic equipment and couriers of cryptographic material.

Section 38
Performance of cryptographic protection

(1) The performance of cryptographic protection means

a) its security administration;
b) specific operation of a cryptographic equipment;
c) production of key material

(2) The performance of cryptographic protection shall be the task of the cryptographic protection officer who is

a) charged with the cryptographic protection by the responsible person;
b) a holder of valid PSC;
c) a holder of a certificate of a Specific Specialist Competence of the cryptographic protection officer (hereinafter “the Specialist Competence Certificate”).

Section 39
Specific specialist competence of a cryptographic protection officer and a specific specialist competence exam

(1) Specific specialist competence of a cryptographic protection officer (hereinafter “the Specific Specialist Competence”) will be verified by a Specific Specialist Competence exam (hereinafter “the Specialist Exam”) and will be proved by the Specialist Competence Certificate.

(2) Specific Specialist Competence involves a complex knowledge of legal and operation regulations and security standards from the area of classified information cryptographic protection, and the ability to implement it.

(3) The Specialist Exam will verify the level of theoretical and working knowledge according to paragraph 2.

(4) The Specialist Exam will be passed on to the Authority or on to the State body delegated by the Authority [S. 137 (q)] at the board of examiners. The board of examiners will be designated by the Director of the Authority or by the responsible person of the delegated State body, and it is composed of three members including its chairman.

(5) An application for a Specialist Exam shall be submitted in writing by the responsible person of the State body or of the facility with the Authority or with the State body delegated by the Authority that shall keep records of applications according the date of delivery. The Specialist Exam shall be passed within six months from the date of submission of application. The Authority or the State body delegated by the Authority shall notify in writing the individual who submitted the Specialist Exam application of the date and place of the Specialist Exam; the notification shall be sent 20 days prior to the date of Specialist Exam at the latest. Any person who fails an exam may repeat it. The repeated exam can be taken only after five working days from the date of an unsuccessful exam.

(6) A Specialist Competence Certificate will be issued by the Authority or by the State body delegated by the Authority for the period of five years. The Authority or the State body delegated by the Authority shall keep records of these certificates.

(7) A contract to perform Specialist Exams and to grant the Specialist Competence Certificates may be made between the Authority and the State body according to S. 52, i.e. the contract for providing these services.

Section 40
Operation of the cryptographic equipment

(1) Operation of the cryptographic equipment means performance of user functions of the cryptographic equipment.

(2) Operators who operate the cryptographic equipment according to paragraph 1 shall

a) be entrusted with the operation by the responsible person or by the individual authorised by the responsible person;
b) meet conditions for access to classified information according to S. 6 par. 1 or S. 11 par. 1; and
c) be trained to be able to operate the cryptographic equipment.

Section 41
Manipulation of cryptographic material

(1) Manipulation of cryptographic material means the form of transmission, transportation, lending, storing or another manner of handling of cryptographic material including its discarding.

(2) Cryptographic material may be recorded and handled only in a manner and by means ensuring that the cryptographic material is protected and that requirements determined by implementing legal regulation will be met.

Section 42
Transportation of cryptographic material and export of cryptographic equipment

(1) A courier of cryptographic material shall carry out transportation of cryptographic material. The courier of cryptographic material shall be the person who

a) was assigned to transport the cryptographic material by the responsible person;
b) is a holder of valid PSC, at least at the same security classification level as that of the cryptographic material being transported;
c) was trained for the transportation.

(2) Transportation of cryptographic material classified TOP SECRET, SECRET and CONFIDENTIAL shall be provided by the courier of cryptographic material accompanied at least by one person who shall be assigned by the responsible person to accompany the courier or by a person authorised by the responsible person to assign the accompanying person and who shall be briefed by the courier on the method and means of transportation.

(3) Export of the certified cryptographic equipment [S. 46 par. 1 (c)] from the territory of the Czech Republic shall be subject to the licence of the Authority. Utilization of the certified cryptographic

equipment by the State body outside the territory of the Czech Republic will not be considered to be an export.

(4) Licence according to paragraph 3 can be granted upon written request. The licence shall be granted for export of specific cryptographic equipment and it shall also contain the purpose of export. No licence will be granted by the Authority if the export would endanger classified information of the Czech Republic or classified information that the Czech Republic has undertaken to protect; the Authority shall report this fact to the applicant. No claim can be laid to the granting of licence.

(5) The Authority shall keep records of licences granted according to paragraph 3.

Section 43
Compromise of the cryptographic material

(1) Compromise of cryptographic material means such handling of cryptographic material that resulted or could result in breach of protection of classified information.

(2) Compromise of cryptographic material shall be immediately reported to the Authority by the State body, legal person or natural person pursuing business.

Section 44
Delegating provisions

Implementing legal regulation shall determine

a) elements of the application for the Specialist Exam;
b) details of composition and actions of the board of examiners;
c) method of performance, organization and classification of the Specialist Exam;
d) format of the Specialist Competence Certificate;
e) minimum requirements for ensuring the security administration of the cryptographic protection;
f) details of providing operation of the cryptographic equipment;
g) method of training of operators of the cryptographic equipment and of the courier of cryptographic material and the format of confirmation of training of the operator of the cryptographic equipment and of the courier of cryptographic material;
h) details of the method of marking elements on classified information in the area of cryptographic protection, particularly according to the type of the cryptographic material;
i) types and elements of administrative aids of the cryptographic protection and requirements for maintaining these aids;
j) detailed requirements for method and for means of handling of cryptographic material;
k) content of application for granting export licence for export of certified cryptographic equipment from the territory of the Czech Republic and elements of the licence.

Section 45
Compromising electromagnetic emissions

(1) Compromising electromagnetic emissions means electromagnetic emissions of electrical and electronic devices that could result in leakage of classified information classified TOP SECRET, SECRET or CONFIDENTIAL.

(2) Protection of classified information from leakage by compromising electromagnetic emissions means securing of electrical and electronic devices, security area or premises.

(3) If the protection of classified information from leakage by compromising emissions is to be provided by a shielded chamber, the Authority must certify this chamber [S. 46 par. 1 (e)].

(4) Shielded chamber means a closed electromagnetically shielded space that prevents electromagnetic emissions from propagation outside this space.

(5) Verification of capability of electrical and electronic devices, security area or premises to protect classified information from the leakage by compromising electromagnetic emissions shall be provided by the Authority during certification of Information System or of the cryptographic equipment or on the basis of written request from the State body or facility.

(6) Contract can be made between the Authority and the State body or facility according to S. 52 for taking measurements of possible leakage of classified information as outlined in paragraph 5, i.e. the contract for providing these services.

(7) The Intelligence Services are qualified to take measurements of device, security area or premises as outlined in paragraph 5 that are operated or used by Intelligence Services. In these cases no contract according to S. 52 will be required. For the

purpose of certification of Information Systems or cryptographic equipment the Intelligence Services will provide the report on the measurement taken including its results to the Authority.

(8) When conducting measurements according to paragraph 7 the Intelligence Services shall comply with provisions of this Act, implementing legal regulations and security standards of the Authority.

Chapter IX
Certification

Section 46
Common provisions

(1) Certification means the procedure whereby the Authority

a) verifies the capability of technical means to protect classified information;
b) verifies the capability of Information System to handle classified information;
c) verifies the capability of the cryptographic equipment to protect classified information;
d) verifies the capability of cryptographic sites to perform activities according to S. 37 par. 6; or
e) verifies the capability of shielded chambers to protect classified information.

(2) When the Authority is satisfied that conditions of capability according to paragraph 1 have been met, it will issue a technical means certificate, information system certificate, cryptographic equipment certificate, cryptographic site certificate or a shielded chamber certificate.

(3) Certificates according to paragraph 2 shall be the legal instruments.

(4) The following shall be included in the technical means certificate

a) registration number of the certificate;
b) name and type designation of the technical means;
c) identification of the technical means producer by the business firm (hereinafter "the Firm") or by name, identification number and location in the case of a legal person, or by name, surname, birth registration number (personal identity number) and permanent residence in the case of a natural person;
d) identification of the holder of the technical means certificate according to (c) above;
e) evaluation of the technical means;
f) date of issue and validity period of the certificate; and
g) official stamp and signature of the authorised representative of the Authority or, if this certificate was issued in the electronic form, electronic signature of the authorised representative of the Authority in accordance with the special legal regulation[22)].

(5) The following shall be included in the Information System certificate, cryptographic equipment certificate, cryptographic site certificate or shielded chamber certificate

a) registration number of the certificate;
b) identification of the holder of the certificate according to paragraph 4 (c);
c) date of issue and validity period of the certificate; and
d) official stamp of the Authority and signature of the authorised representative of the Authority or, if these certificates were issued in the electronic form, electronic signature of the authorised representative of the Authority in accordance with the special legal regulation[22)].

(6) In addition to the elements according to paragraph 5 the Information System certificate shall contain the security classification level of classified information for which the capability of the Information System has been verified.

(7) In addition to the elements according to paragraph 5 the cryptographic equipment certificate shall contain

a) identification of the cryptographic equipment;
b) identification of the cryptographic equipment producer according to paragraph 4 (c); and
c) security classification level of classified information for which the capability of the cryptographic equipment has been approved.

(8) In addition to the elements according to paragraph 5 the cryptographic site certificate shall contain

a) identification and specification of the cryptographic site location; and
b) scope of capability of the cryptographic site.

(9) In addition to the elements according to paragraph 5 the shielded chamber certificate shall contain

a) identification of the shielded chamber for which it has been issued;
b) identification of the shielded chamber producer according to paragraph 4 (c); and
c) security classification level of classified information for which the capability of the shielded chamber has been approved.

(10) If the Authority is not satisfied concerning conditions of capability according to paragraph 1, it shall determine that the certificate will not be granted. No appeal shall be permitted against the decision not to grant a certificate according to paragraph 1 (b) and (c).

(11) The Authority shall decide the termination of validity of the certificate in the cases outlined in S. 47 par. 4 (b), S. 48 par. 4 (d), S. 49 par. 5 (b), S. 50 par. 4 (d) and S. 51 par. 4 (d). An appeal lodged against the decision of the Authority to terminate validity of the certificate has no suspension effect. No appeal shall be permitted against the decision of the Authority to terminate validity of the Information System certificate and the cryptographic equipment certificate.

(12) If validity of the certificate expired or was terminated according to S. 47 par. 4 (b), S. 48 par. 4 (b) and (d), S. 49 par. 5 (b), S. 50 par. 4 (b) and (d), or S. 51 par. 4 b) and d), the certificate holder shall forward the certificate to the Authority, within five days from the date of delivery of the decision of the Authority.

(13) The certification report shall be the Annex of Information System certificate, cryptographic equipment certificate, cryptographic site certificate or shielded chamber certificate that shall contain principles and conditions for their operation. Conditions of the use of technical means may be set forth in the Annex of the technical means certificate.

(14) The Authority shall verify capability of the technical means according to paragraph 1 (a) on the basis of evaluations of technical means parameters (hereinafter "the Evaluations").

(15) The Authority can conclude a contract with the State body or with the facility according to S. 52 for purposes of issuing Evaluations according to paragraph 14 and for purposes of performance of partial tasks in verifying capability according to paragraph 1 (b) to (e); this possibility does not apply to the cases of verification of capability of Information Systems, cryptographic equipment or cryptographic sites or shielded chambers intended to be used by the Intelligence Services.

(16) The list of the State bodies and facilities, with which the Authority concluded a contract according to S. 52, will be published by the Authority in the Bulletin of the Authority.

(17) Only the Intelligence Services concerned are authorised to perform partial tasks in verifying capability according to paragraph 1 (b) to (e) that cannot be performed by the Authority for reasons of confidentiality, where Information Systems, cryptographic equipment, cryptographic sites or shielded chambers are in question, that are intended to be used by these Intelligence Services. In these cases reports shall be forwarded to the Authority by the Intelligence Services on performance of partial tasks including results.

(18) In performing partial tasks according to paragraph 17 the Intelligence Services shall comply with provisions of this Act, implementing legal regulations and security standards of the Authority.

(19) The requesting subject according to S. 47 par. 1, S. 48 par. 1, S. 49 par. 1, S. 50 par. 1 and S. 51 par. 1 shall be the party of the certification procedure or certificate revoking procedure.

Section 47
Request for technical means certification and validity of the technical means certificate

(1) The producer, importer, distributor or user of the technical means shall request a technical means certification in writing with the Authority. Evaluations according to S. 46 par. 14 and the documentation necessary to carry out the technical means certification shall be enclosed in the request.

(2) The validity period of the technical means certificate shall be determined by the Authority for no longer than five years.

(3) The list of certified technical means will be published in the Bulletin of the Authority, with the exception of technical means certified upon request of the user of technical means.

(4) Validity of the technical means certificate shall terminate

a) upon expiration of its validity period; or
b) by decision of the Authority on termination of the certificate validity if the technical means

being produced fail to comply with requirements of this Act and with implementing legal regulations or if it is not identical to the technical means being evaluated.

(5) If validity of the technical means certificate was terminated according to paragraph 4, the Authority will remove this technical means from the list published in accordance with paragraph 3.

(6) The technical means used for the protection of classified information may continue to be used even after expiration of its certificate validity period.

(7) During the process of the technical means certification, the certificate or similar document of the technical means issued by authorised professional department of a foreign power can also be taken into account by the Authority.

Section 48
Request for Information System certification and validity of the Information System certificate

(1) Information System certification shall be requested in writing with the Authority by the State body or by the facility that will operate the Information System.

(2) During the process of certification, a subject that requested for the Information System certification according to paragraph 1 shall submit all documents necessary for carrying out certification at the request of the Authority.

(3) The Authority shall determine the validity period of the Information System certificate. Depending on the security level the validity of the Information System certificate shall not extend beyond

a) two years for TOP SECRET and SECRET;
b) three years for CONFIDENTIAL; and
c) five years for RESTRICTED.

(4) Validity of the Information System certificate shall terminate

a) upon expiry of its validity period;
b) upon termination of validity of the FSC;
c) upon dissolution of the State body; or
d) by decision of the Authority on termination of the certificate validity if the Information System ceased to be applicable for handling classified information.

(5) Where the Information System is to be used also immediately after expiration of the validity period of its certificate, the requesting subject according to paragraph 1 shall request the Authority to provide certification of the Information System. Repeated requests shall be forwarded to the Authority at least six months before the expiration of a validity period of the original Information System certificate.

(6) The Authority shall take a decision on Information System certification within one year of initiation of the certification process, for more complex cases within two years; if the case cannot be decided within this period with respect to its nature, the director of the Authority may reasonably extend the period, but not by more than six months.

Section 49
Request for the cryptographic equipment certification and validity of the cryptographic equipment certificate

(1) The producer, importer, distributor or user of the cryptographic equipment shall request the cryptographic equipment certification in writing with the Authority. If the facility requests cryptographic equipment certification, it shall be the holder of the valid FSC for access to classified information according to S. 20 par. 1 (a).

(2) The Authority shall reject the request according to paragraph 1 by its decision if it is not in line with the intentions of the Czech Republic in the area of providing protection of classified information by cryptographic protection. No appeal shall be permitted against the decision according to the first sentence and this decision cannot be re-examined by the court.

(3) During the process of certification, the subject that requested the cryptographic equipment certification according to paragraph 1 shall submit the necessary number of units of the cryptographic equipment, as well as the documentation necessary for carrying out the certification, at the request of the Authority.

(4) The validity period of the cryptographic equipment certificate shall be determined by the Authority for no longer than five years.

(5) The validity of the cryptographic equipment certificate shall terminate

a) upon expiry of its validity period; or

b) by decision of the Authority on termination of the certificate validity if the cryptographic equipment ceased to be applicable for the protection of classified information.

(6) Where the cryptographic equipment is to be used also immediately on the expiry of the validity period of its certificate, the requesting subject according to paragraph 1 shall request the Authority to provide certification of the cryptographic equipment. Repeated requests shall be forwarded to the Authority at least six months before the expiration of a validity period of the original cryptographic equipment certificate.

(7) During the process of the cryptographic equipment certification the Authority may take into account the certificate or similar document of the cryptographic equipment issued by the authorised professional office of a foreign power.

(8) The process of certification of the cryptographic equipment can also be suspended at the moment of sending of the request addressed to the foreign subject for information that is necessary for positive determination of the status of a case.

(9) S. 48 par. 6 shall apply for the time limits laid down for issue of the decision.

Section 50
Request for cryptographic site certification
and validity of the cryptographic site certificate

(1) Cryptographic site certification shall be requested in writing with the Authority by the State body or by the facility that should operate the cryptographic site. If the facility requests cryptographic site certification, it shall be the holder of a valid FSC.

(2) The subject that requested the cryptographic site certification according to paragraph 1 shall submit documents necessary for carrying out the certification during the process of certification at the request of the Authority.

(3) The validity period of the cryptographic site certificate shall be determined by the Authority for no longer than three years.

(4) The validity of the cryptographic site certificate shall terminate

a) upon expiry of its validity period;
b) upon termination of validity of the FSC;
c) upon dissolution of the State body; or
d) by decision of the Authority on termination of the certificate validity if the cryptographic site ceased to be applicable to perform assigned activities.

(5) Where the cryptographic site is to be used immediately on the expiry of the validity period of its certificate, the requesting subject according to paragraph 1 shall request the Authority to provide the certification of the cryptographic site. Repeated requests shall be forwarded to the Authority at least six months before the expiration of a validity period of the original cryptographic site certificate.

(6) The Authority shall take a decision on cryptographic site certification within six months of the initiation of the certification process, in very complex cases within one year; if the case cannot be decided within this period, with respect to its nature, the director of the Authority may reasonably extend the period, but not by more than three months.

Section 51
Request for shielded chamber certification
and validity of the shielded chamber certificate

(1) Shielded chamber certification shall be requested in writing with the Authority by the State body or by the facility that uses the shielded chamber.

(2) The subject that requested the shielded chamber certification according to paragraph 1 shall submit documents necessary for carrying out the certification during the process of certification at the request of the Authority.

(3) The validity period of the shielded chamber certificate shall be determined by the Authority for no longer than five years.

(4) Validity of the shielded chamber certificate shall terminate

a) upon expiry of its validity period;
b) upon termination of validity of the FSC;
c) upon dissolution of the State body; or
d) by decision of the Authority on termination of the certificate validity if the shielded chamber ceased to be applicable for protection of classified information.

(5) Where the shielded chamber is to be used also immediately on the expiry of the validity period of its certificate, the requesting subject according to paragraph 1 shall request the Authority to provide

certification of the shielded chamber. Repeated requests shall be forwarded to the Authority at least 12 months before the expiration of a validity period of the original shielded chamber certificate.

(6) S. 50 par. 6 shall apply for the time limits laid down for issue of the decision.

Section 52
Contract for providing services

(1) A contract for providing services (hereinafter "the Contract") mentioned in S. 39 par. 7, S. 45 par. 6 and S. 46 par. 15 will be concluded for a fixed term or for indefinite period of time. The Contract shall be drawn up in writing. A declaration of will of contracting parties must be on the same document.

(2) The Contract can be concluded with the State body or with the facility upon their written request on the condition that the activities that are the subject matter of a Contract

a) will be carried out by professionally qualified state or facility employees;
b) will be provided on the part of the State body or facility organizationally, technically and materially.

(3) The Contract with a facility can be concluded only if the facility

a) is located or incorporated on the territory of the Czech Republic;
b) is a holder of the valid FSC for the appropriate security classification level; this condition does not apply if the Contract should be concluded for issuing Evaluations as outlined in S. 46 par. 15.

(4) The Contract shall contain

a) identification of contracting parties;
b) specification of the subject matter of the Contract and of its scope;
c) rights and obligations of contracting parties;
d) method of control conducted by the Authority according to paragraph 6;
e) method and conditions of withdrawal from the Contract by contracting parties;
f) consent to publication of technical means in the Bulletin of the Authority in the case of Contracts for issuing Evaluations as outlined in S. 46 par. 15.

(5) Conditions according to paragraph 4 (e) shall include the stipulation that the Authority will withdraw from the Contract if the other contracting party breaches a duty specified in this Act, implementing legal regulations or in the Contract concluded.

(6) The Authority shall verify whether the other contracting party complies with the terms of the Contract, implementing legal regulations and the contract concluded.

(7) The content of the Contract may be changed only by written agreement of contracting parties.

(8) The Contract may be terminated only in writing.

(9) In other cases provisions of the Commercial Code will be adequately applied, unless otherwise provided herein.

Section 53
Delegating provisions

Implementing legal regulation shall stipulate

a) the elements of the request for technical means certification, Information System certification, cryptographic equipment certification, cryptographic site certification and shielded chamber certification;
b) the elements of the repeated request for Information System certification, cryptographic equipment certification, cryptographic site certification and shielded chamber certification;
c) the documents necessary for conducting technical means certification, Information System certification, cryptographic equipment certification, cryptographic site certification and shielded chamber certification;
d) the formats of technical means certificate, Information System certificate, cryptographic equipment certificate, cryptographic site certificate and shielded chamber certificate;
e) the rules for determining the validity period of the technical means certificate;
f) the rules and method of application of technical means on the expiry of the validity period of its certificate;
g) the method and conditions for conducting Information System certification, cryptographic equipment certification, cryptographic site certification and shielded chamber certification and its repetition;
h) the content of the certification report according to S. 46 par. 13;

i) the elements of the request for verification of electrical and electronic devices capability, security area capability or premises capability to protect classified information from leakage by compromising electromagnetic emissions, as well as the method of evaluation of their capability; and
j) the elements of the request of the State body or facility for conclusion of a Contract according to S. 52.

Chapter X
Personnel security clearance, facility security clearance, special access and release from the obligation to maintain confidentiality

Personnel security clearance and facility security clearance
Section 54

(1) The PSC and the FSC shall be the legal instruments.

(2) The PSC shall contain

a) name, surname, maiden name;
b) day, month, year of birth, birthplace;
c) birth registration number (personal identity number);
d) nationality;
e) the highest security classification level of classified information to which the PSC gives access;
f) date of issue and validity period;
g) official stamp and signature of the authorised representative of the Authority or, if this security clearance was issued in the electronic form, electronic signature of the authorised representative of the Authority in accordance with the special legal regulation[22)].

(3) The FSC shall contain

a) identification of the facility by firm or name, identification number and location in the case of a legal person, in the case of a natural person data according to paragraph 2 (a) to (d);
b) highest security classification level of classified information to which the FSC gives access;
c) the form of access according to S. 20;
d) date of issue and validity period;
e) official stamp and signature of the authorised representative of the Authority or, if this security clearance was issued in the electronic form, electronic signature of the authorised representative of the Authority in accordance with the special legal regulation[22)].

Section 55

(1) Period of validity of the PSC and the FSC shall be as follows

a) TOP SECRET five years;
b) SECRET seven years;
c) CONFIDENTIAL nine years;

(2) Period of validity of the FSC for security classification level RESTRICTED shall be 12 years.

Section 56

(1) Validity of the PSC or the FSC shall terminate

a) upon expiry of its validity period;
b) on the date of enforcement of decision of the Authority (S. 123 par. 3, S. 126 par. 4) to terminate its validity (S. 101);
c) upon death of natural person or upon declaration the natural person death;
d) upon dissolution or cessation of existence of the facility;
e) upon notification of its loss or theft;
f) as a result of the damage to the extent resulting in illegibility of records in the document or causing the breach of its completness;
g) as a result of a change to data contained therein;
h) upon formation of service relationship as a member of the Intelligence Service or employment relationship of an employee placed in the Intelligence Service in the case of a personnel security clearance issued by the Authority;
i) upon the end of the service relationship of the member of the Intelligence Service or employment relationship of the employee who is placed in the Intelligence Service, or on the date, when the natural person ceases to be the person as outlined in S. 141 par. 1, in the case of a personnel security clearance issued by the Intelligence Service concerned or by the Ministry of the Interior.

(2) When the validity of the FSC ends according to paragraph 1 (a), (b) and (d), the facility shall forward the provided classified information to the providing body or to the body having the jurisdiction over classified information; if this practice cannot be complied with, it shall forward this classified

information to the Authority. Classified information originated by the facility shall be forwarded by the facility to the State body having the jurisdiction over classified information, if there is no such State body, it shall be forwarded to the Authority. Classified information shall be transferred and forwarded by the facility according to this paragraph immediately after termination of validity of the FSC.

(3) When the validity of the PSC ends according to paragraph 1 (a) and (b), the responsible person or an individual who conducted the briefing shall prevent the natural person concerned from having access to classified information.

(4) Access of a natural person or facility to classified information will not be affected by termination of the validity of the PSC or the FSC according to paragraph 1 (e) to (g); in this case the Authority shall issue, upon written request, a new security clearance that replaces the original security clearance, within five days from the delivery of the request.

Section 56a

(1) In the case of termination of validity of the personnel security clearance according to S. 56 par. 1(h), a new PSC will be granted to that natural person by the Intelligence Service concerned, which supersedes the original security clearance, on the date of formation of their service relationship or employment relationship.

(2) In the case of termination of validity of the personnel security clearance according to S. 56 par. 1(i), the natural person concerned will be issued with a new PSC, which supersedes the original security clearance, by:

a) the Intelligence Service concerned, on the date of formation of service relationship as a member of the Intelligence Service or employment relationship of an employee placed in the Intelligence Service;
b) the Ministry of the Interior, on the date when the natural person concerned became the person as outlined in S. 141 par. 1; or
c) the Authority in any other case, on the date following the date of termination of validity of the original security clearance. The Authority will issue a new personnel security clearance upon written request of the person concerned within five days of the service of an application. The application for issuance of the new personnel security clearance may be submitted within 30 days of the termination of validity of the original security clearance; a confirmation of the Intelligence Service concerned or confirmation of the Ministry of the Interior according to paragraph 3 shall be enclosed to the application.

(3) In the case of procedure according to paragraph 2(c) the Intelligence Service concerned or the Ministry of the Interior will confirm the termination of validity of a personnel security clearance upon request of that natural person, within five days of the service of the request. The name of the State body shall be entered in the confirmation, which had issued the original personnel security clearance, as well as data according to S. 54 par. 2(a)-(f) and the date of termination of this clearance.

(4) A State body, which issued a new personnel security clearance, shall request in writing a security file of that person from the State body, which had issued the original security clearance; the security file will be forwarded within five days of the service of the request.

Section 57
Personnel security clearance for a foreign power and facility security clearance for a foreign power

(1) Upon the written request of the natural person or responsible person of the legal person pursuing business the Authority will issue

a) the PSC for a foreign power; or
b) the FSC for a foreign power.

(2) The security clearance according to paragraph 1 shall be the legal instrument.

(3) The security clearance according to paragraph 1 shall contain elements outlined in S. 54, and the marking of the highest security classification level of classified information to which this security clearance gives access shall be indicated including the abbreviation as determined by S. 21 par. 2.

(4) The security clearance according to paragraph 1 certifies that its holder has been security cleared according to Part four and that he is a holder of the valid PSC or FSC of the given security classification level; it certifies as well, in the case of FSC, forms of access of the facility to classified information according to S. 20.

(5) The security clearance according to paragraph 1 shall be issued only for the necessary

period of time but for no longer than the period for which the PSC or the FSC has been issued.

(6) When the validity of the PSC or the FSC ends, save where the validity of the clearance ends according to S. 56 par. 1 (e) and (f), then also the validity of the security clearance outlined in paragraph 1 shall be terminated.

(7) The validity of the security clearance according to paragraph 1 shall also be terminated by reason of damage to the extent resulting in illegibility of records or causing the breach of its completness, or upon notification of its theft or loss.

(8) The holder of the security clearance according to paragraph 1, the validity of which was terminated according to paragraph 6, shall hand it over to the Authority within five days.

Special access to classified information
Section 58

(1) The following persons may have access to classified information, irrespective of the classification of the information, without the valid PSC and briefing

a) president of the Czech Republic;
b) Deputies and Senators of the Parliament;
c) Members of the Government;
d) Ombudsman and Deputy Ombudsman
e) judges; and
f) president, vice-president and members of Supreme Audit Office.

(2) Persons listed in paragraph 1 shall have access to classified information as from the date of election or appointment to an office to the extent necessary for its discharge.

(3) Access to classified information without valid PSC may be granted to a natural person acting on behalf of the Intelligence Service[24)], to an informant[25)] or to a natural person who was afforded special protection according to the special legal regulation[26)], or to the member of the Intelligence Service, who is assigned to the special reserve[27)]. The subject that granted access to classified information shall conduct the briefing of this person. This person concerned may not be granted access to classified information of a foreign power.

(4) The special legal regulation[28)] stipulates which natural persons and under what conditions may have access to classified information without the valid PSC during criminal proceedings, civil legal proceedings and legal administrative proceedings to the extent necessary to claim their rights and to fulfil their duties within the frame of these proceedings. In these cases access to classified information may be granted only after a briefing conducted according to paragraph 5.

(5) The individual determined by the special legal regulation[28)] shall conduct the briefing according to S. 2 (i) of persons listed in paragraph 4. The briefing shall be conducted reasonably as outlined in S. 9 par. 1; further the briefing shall contain the file marking of the case that is the subject-matter of the proceedings, as well as instruction that the data concerning persons having access to classified information according to paragraph 4 are recorded by the Authority and can be used as described herein.

(6) With the exception of the President of the Czech Republic, President of the Senate of the Parliament of the Czech Republic, Speaker of the Chamber of Deputies of the Parliament of the Czech Republic, Prime Minister and Minister of foreign affairs, persons mentioned in paragraphs 1 and 4 may not have access to classified information of a foreign power.

Section 59
One-time access to classified information

(1) Upon written request of the responsible person the Authority may exceptionally and in justified cases issue its consent to access on a one-time basis to classified information classified one level higher than that to which the valid PSC or FSC has been issued, for the necessary period of time but for no longer than six months.

(2) Consent according to paragraph 1 may be granted to the facility only for access to classified information according to S. 20 par. 1 (b).

(3) Consent to one-time access according to paragraph 1 for members of Intelligence Services can be given by the director of the Intelligence Service in question, and for the Police members according to S. 141 par. 1 by the Minister of the Interior, upon written request of the appropriate service officer.

(4) Request according to paragraph 1 shall contain

a) justification of one-time access;

b) identification of field of classified information to which one-time access should be granted;
c) the copy of the PSC or the FSC;
d) required time period of one-time access;
e) in the case of facility, written approval of the provider of classified information to give consent according to paragraph 1.

(5) The Authority shall issue consent according to paragraph 1 without delay within five days from the delivery date of the request. The responsible person who determines after the consent of the Authority that the natural person can be granted access to classified information according to paragraph 1 or 3 shall conduct a briefing of that person.

(6) No legal claim can be laid to the granting of consent to one-time access to classified information and it can be granted only once to the same person.

(7) One-time access to classified information of a foreign power may be granted only in accordance with requirements of the foreign power concerned.

Section 60

(1) In the case of participation of the Czech Republic in an international armed conflict or in international rescue or humanitarian mission, in the case of a declaration of belligerency and in the case of a state of danger, emergency or state of endangering of the State[20)] access to classified information may be granted to the natural person who is not a holder of a PSC or has not access to classified information at the level RESTRICTED, or to the facility that is not a holder of a FSC.

(2) Access to classified information according to paragraph 1 may be granted to the natural person only if his/her trustworthiness and ability to keep confidentiality of information are undisputed.

(3) In the case of access according to paragraph 1 the responsible person shall arrange a briefing of the natural person. If there is a danger of delay or by reason of other types of urgency and importance of specific task, the briefing may be replaced by a verbal familiarisation of the natural person with his/her responsibilities in the area of protection of classified information and with consequences that the law or administrative or executive order provides in the case of their breach.

(4) A responsible person shall make a written record of access according to paragraph 1. The responsible person shall forward this written record immediately together with the briefing to the Authority; if the briefing has been replaced by the verbal familiarisation according to paragraph 3, second sentence, reference shall be made in the written record. If the Intelligence Service has granted the access, neither the written record according to the first sentence and according to the part of the second sentence after semicolon, nor the briefing, will not be forwarded to the Authority, but the Intelligence Service in question will retain them.

(5) When facility is granted access according to paragraph 1, its responsible person shall make a written record thereof that shall be immediately forwarded to the Authority.

(6) In emergency the access to classified information of a foreign power may only be granted in accordance with requirements of the foreign power concerned.

Section 61

One-time access to classified information according to S. 59 and access according to S. 60 cannot be granted in the case of classified information TOP SECRET or to classified information subject to the Special Handling Regime.

Section 62
Access to classified information on the basis of recognition of the security authorization issued by the authority of a foreign power

(1) Access to classified information can also be granted to the briefed natural person or to the facility in the cases when the Authority recognizes security authorization issued by the authority of a foreign power that has competence to protect classified information (hereinafter "the Security Authorization"). The Authority will recognize the Security Authorization if laid down by an international agreement to which the Czech Republic is bound. Further, the Authority may recognize the Security Authorization if this recognition is in accordance with foreign policy and security interests of the Czech Republic; nevertheless no legal claim can be laid to this recognition. When acting according to the third sentence, the Authority can request the opinion of the Ministry of Foreign Affairs and of the corresponding Intelligence Service; if the Authority does not receive the requested standpoint within 30 days of the service of the request than it can have reasonable cause to believe that the standpoint is affirmative.

(2) Recognition according to paragraph 1 will be applied by the Authority upon request of the natural person not pursuing business or of the facility that are holders of the Security Authorization. The request shall contain the following

a) name, surname and university degree of the Security Authorization holder;
b) date and place of birth and permanent residence address of the Security Authorization holder;
c) nationality of the Security Authorization holder;
d) in the case of facility its identification by the firm or name, identification number and location in the case of a legal person, or identification by the name, surname and permanent residence address in the case of a natural person;
e) reason why recognition according to paragraph 1 should be applied;
f) required validity period of the recognition;
g) signature of the Security Authorization holder and delivery address of the recognition according to paragraph 1.

(3) Official translation of the Security Authorization shall be attached to the request according to paragraph 2 or its authenticated copy.

(4) The Authority will send the recognition according to paragraph 1, the second sentence, to the Security Authorization holder within 10 days of the date of submission of the request. The Authority will send the recognition according to paragraph 1, the third sentence, to the Security Authorization holder within 60 days of the date of submission of the request. If the recognition is not in accordance with foreign policy and security interests of the Czech Republic, the Authority will not affirmatively dispose of the request and notify the applicant in writing thereof within the same time limit.

(5) Recognition according to paragraph 1 shall contain the following

a) data according to paragraph 2 (a) to (d);
b) identification of the Security Authorization, which was issued by the authority of a foreign power;
c) marking of the highest security classification level of classified information to which the recognition according to paragraph 1 gives access;
d) in the case of facility the form of access according to S. 20;
e) date of issue and validity period;
f) official stamp and signature of the authorised representative of the Authority or, if this recognition was issued in the electronic form, the electronic signature of the authorised representative of the Authority in accordance with the special legal regulation[22)].

Release from the obligation to maintain confidentiality
Section 63

(1) In proceedings before the State body, upon the request of this body, the responsible person of the State body having the subject-matter jurisdiction over classified information may release the natural person from the obligation to maintain confidentiality (hereinafter "the Release from Confidentiality"), unless otherwise provided herein (paragraph 8 and S. 133 par. 2).

(2) In the case of cessation of existence of the State body without the legal successor the Release from Confidentiality may be made by the director of the Authority.

(3) For the purpose of proceedings according to paragraph 1 the Release from Confidentiality will be further made by

a) President of the Republic with respect to the Prime Minister, President, Vice-President and members of the Supreme Audit Office, President and deputy President of the Constitutional Court, President and deputy President of the Supreme Court, President and deputy President of the Supreme Administrative Court, Head of the Office of the President of the Republic, Ombudsman, deputy Ombudsman, Governor and deputy Governors of the Czech National Bank;
b) Chamber of Deputies with respect to Deputies;
c) Senate with respect to Senators;
d) Speaker of the Chamber of Deputies with respect to the Head of Office of the Chamber of Deputies;
e) President of the Senate with respect to the Head of Office of the Senate;
f) Prime Minister with respect to ministers and heads of other central administrative offices;
g) President of the Constitutional Court with respect to the Constitutional Court Justice;
h) Minister of Justice with respect to judges not set out under (g) above, prosecuting attorneys and lay judges, and the Government with respect to Director of the Security Intelligence Service.

(4) If the obligation to maintain confidentiality concerns the subject-matter discussed by the body of the Parliament, the Chamber of Deputies or Senate

can make the Release from Confidentiality after obtaining the opinion of the responsible person of the State body having the subject-matter jurisdiction over classified information.

(5) Prior to the Release from Confidentiality according to paragraph 3 the responsible person of the State body having the subject-matter jurisdiction over classified information shall be asked for his/her opinion.

(6) No Release from Confidentiality will be required in the case of the President of the Republic.

(7) The Release from Confidentiality only applies to classified information in question to the extent as is considered necessary and only as long as this is necessary. The Release from Confidentiality shall be made in writing. Security classification of classified information is not affected by the Release from Confidentiality.

(8) The Release from Confidentiality may be denied in the cases where it could result in extremely serious detriment to the interest of the Czech Republic or where life and limb of persons could be put in jeopardy.

Delegating provision
Section 64

Implementing legal regulation shall determine the following

a) the PSC format and the FSC format;
b) format of request for issuance the PSC for the foreign power and format of request for issuance the FSC for the foreign power;
c) format of requests for recognition of personnel Security Authorization and facility Security Authorization.

Chapter XI
Obligations in protection of classified information

Section 65
Common obligations

(1) Each individual shall forward immediately any classified information found or obtained contrary to this Act, or a PSC, FSC, PSC for a foreign power or FSC for a foreign power (hereinafter "the Document Found") to the Authority, Police or to the Embassy of the Czech Republic.

(2) Each individual who had or has access to classified information shall hold it in confidence and shall not grant access to it to any unauthorised person.

(3) Each individual who submitted application according to S. 94 shall report to the Authority immediately all changes to the data set out in it.

(4) In performance of the state control by the Authority each individual shall fulfil instructions of the control officer in implementing urgent measures according to S. 144 par. 1.

Section 66
Obligations of the natural person who has access to classified information and obligations of the natural person who is a holder of the personnel security clearance

(1) The natural person who has access to classified information, shall

a) comply with obligations in the protection of classified information;
b) hand over, within five days, to the issuing authority of the PSC, his/her PSC, the validity of which has been terminated according to S. 56 par. 1(b) and (f)-(i);
c) report immediately in writing to the issuing authority of the PSC or PSC for the foreign power, loss or theft of his/her PSC or PSC for the foreign power;
d) report immediately to the Authority changes to data set out in his/her application of the natural person according to S. 94 par. 2 (a), (c) and (d);
e) report immediately to the person who made his/her briefing according to S. 9 par. 1 or S. 11 par. 2 all breaches of obligations determined herein;
f) take part in trainings according to S. 67 par. 1 (b).

(2) The natural person who is a holder of PSC but has not access to classified information will be only under the duties according to paragraph 1 (b) to (d).

Section 67
Obligations of the responsible person

(1) The responsible person shall

a) provide a briefing of the natural person;
b) provide at least an annual training of natural persons who have access to classified information, in the area of legal regulations on the protection of classified information;
c) provide verification whether conditions for access of the natural person to information classified RESTRICTED have been fulfilled;
d) approve the Information System for operation and report this fact in writing to the Authority;
e) authorise the natural person to activities in the field of or to performance of the cryptographic protection;
f) control the fulfilment of other obligations determined herein.

Section 68
Obligations of the facility that is a holder of a facility security clearance

The facility that is a holder of the FSC shall

a) forward to the Authority the FSC within five days of the service of the final decision of the Authority according to S. 101 par. 2, validity of which was terminated by the Authority;
b) report to the Authority, without delay, loss or theft of the FSC or of the FSC for the foreign power;
c) report immediately to the Authority all changes to the data set out according to S. 97 (a) and (b) in the facility security questionnaire;
d) report to the Authority by the 1st November every year all changes to the data set out in the application of the facility according to S. 96 par. 2 (a) and (b) and prove these changes as outlined in S. 96 par. 2 (c);
e) provide protection of classified information where validity of the FSC was terminated,
f) sent to the Authority the decision on the transformation[28a)] of the facility within 15 days from the date of its acceptance.

Section 69
Obligations of the legal person and of the natural person pursuing business who have access to classified information, and obligations of the State body

(1) A legal person and natural person pursuing business who have access to classified information and the State body shall

a) provide protection of classified information according to this Act and according to international agreements;
b) prepare and maintain a review of positions or offices that will necessarily require access to classified information, including classified information of the European Union, North Atlantic Treaty Organisation and classified information requiring Special Handling Regime, together with the security classification level, or positions or offices that may not be discharged without a Specialist Competence Certificate according to this Act (S. 39); without prejudice to provisions of special legal regulations in the field of specialist competence[29)];
c) notify in writing without delay the Authority of any fact that could affect issuance or validity of a PSC or FSC;
d) provide conditions for marking, recording, lending, storing, transportation, other handling and discarding of classified information and classified information subject to a Special Handling Regime in accordance with implementing legal regulation;
e) operate only such an Information System that was certified by the Authority and approved in writing that it can be put in operation;
f) suspend operation of the Information System that does not fulfil conditions set out in certification report and safeguard classified information involved, and inform the Authority thereof;
g) operate only such a Communication System, the security project of which was approved by the Authority;
h) suspend operation of the Communication System that does not fulfil conditions determined in the Communication System security project, and inform the Authority thereof;
i) use only such an equipment for the cryptographic protection that has been certified by the Authority, and utilise the cryptographic site only for purposes, for which it has been certified and approved for operation;
j) maintain records of natural persons who have access to classified information, records of

cryptographic material, records of the cryptographic protection staff, records of the cryptographic equipment operators; records of couriers of the cryptographic material and records of unauthorised handling of classified information;

k) report to the Authority any breach of obligations in protection of classified information or obligation imposed by the international agreement in the area of protection of classified information and implementation of remedial and corrective measures; this obligation does not apply to the Intelligence Services in the cases according to S. 140 par. 1 (a) and to the Ministry of the Interior in the cases according to S. 141 par. 1, with the exception of breach of protection of classified information of the North Atlantic Treaty Organization or of the European Union;
l) establish the registry of classified information being provided (S. 79) and report changes in this registry to the Authority to the extent determined by the implementing legal regulation;
m) at least annually carry out an inventory of classified information maintained in the registry of classified information, which has been provided during the past calendar year and notify the Authority of the result, together with the number of classified information and its classification levels; this notification will not be forwarded by the Intelligence Services;
n) forward any classified information released by the foreign power or by the foreign partner of the legal person or of the natural person pursuing business, to be recorded by the Authority or by the Ministry of the Foreign Affairs according to S. 79 par. 4;
o) release in the cases determined by this Act classified information of the foreign power through the central registry (S. 79 par. 2);
p) ensure that the natural person will be authorised in writing to have access to classified information with the Special Handling Regime marked as "ATOMAL";
q) inspect whether other obligations determined by this Act are complied with.

(2) The obligation set out in paragraph 1 (c) does not apply to the Intelligence Services in the cases according to S. 140 par. 1 (a) and to the Ministry of the Interior in the cases according to S. 141 par. 1.

Section 70
Obligations in the protection of industrial property

(1) Any person who submits to the Office of Industrial Property invention application, utility design application or topography of a semiconductor product application (hereinafter "the Applicant") shall mark on the application the proposal of the security classification level, when it appears to him/her that the subject-matter of the application contains classified information. When the Applicant is the legal person, it shall state in the application the name, surname and position or office of the responsible person.

(2) The Office of Industrial Property shall submit the application according to paragraph 1 to the Authority that, upon receiving the opinion of the central administrative office having the subject-matter jurisdiction over the subject of the application, confirms the proposal of the classification level, changes it or, if the subject of the application does not involve classified information, denies the proposal; if the subject of the application falls within the subject-matter jurisdiction of no central administrative office, no opinion will be required.

(3) The Authority shall report confirmation or change to the proposal for the security classification level in accordance with paragraph 2 to the Office of Industrial Property within a period of 60 days from the date of delivery of the application to the Authority, or it will give it a notice within the same period that it denied proposal for the security classification and return the application to the Office of Industrial Property; at the same time the Authority shall state in the notification whether the Applicant meets conditions for access to classified information.

(4) The Office of Industrial Property shall mark security classification level notified according to paragraph 3 on the application and announce it immediately to the Applicant who shall mark the security classification level as described (S. 21 and 22) on the subject of the application; if the Applicant is a natural person not pursuing business, the Office of Industrial Property will have the position of the originator. The Office of Industrial Property will also forward notification according to paragraph 3 immediately to the Applicant.

(5) If the subject of application according to paragraph 1 contains classified information and the Applicant does not meet conditions for access to classified information of this security classification level, the Office of Industrial Property shall conduct

his/her briefing, if the Applicant is a natural person, and if the Applicant is a legal person, the briefing shall be conducted of the responsible person of the Applicant; the responsible person of the Applicant shall brief all natural persons who had access to the subject of application within the frame of the legal person of the Applicant or who necessarily need it; on the basis of the briefing these persons will be considered to be persons who fulfil conditions for access to classified information involved in the subject of application. Provisions of S. 9 par. 1, last sentence, and S. 11 par. 2, third sentence, will apply similarly.

Section 71
Security director (security officer)

(1) The State body that creates classified information or to that classified information has been provided, and further the legal person and the natural person pursuing business who have access to classified information, shall establish and staff the position of the security director (security officer). The position of the security director (security officer) can be carried out by the responsible person him/herself; otherwise the security director (security officer) is directly inferior in authority to the responsible person.

(2) The State body, legal person and natural person pursuing business according to paragraph 1 shall report in writing within 15 days from staffing the position of the security director (security officer) to the Authority the name, surname and birth registration number (personal identity number) of the person holding this position.

(3) The security director (security officer) shall ensure and fulfil duties laid on him/her in writing by the responsible person as set out herein; the liability of the responsible person for the protection of classified information shall not be affected by the appointment of the security director (security officer).

(4) The position of the security director (security officer) can be held only be the natural person who fulfils conditions for access to classified information of such security classification, to which he/she will have access in exercising his/her office.

(5) The position of the security director cannot be held for more State bodies or facilities simultaneously.

Section 72
Personnel project

(1) Ministries and other central administrative offices shall prepare a personnel project every year.

(2) The personnel project shall contain

a) an analysis of the situation in the field of personnel security in the past year;
b) the assumed number of natural persons who will have to be cleared in the next year according to S. 92 (a) for various security classification levels.

(3) Ministries and other central administrative offices will send the personnel project to the Authority annually by the 31st October of the corresponding calendar year.

(4) The Authority will forward personnel projects together with its opinion to the Government by the 30th November of the corresponding calendar year for approval.

Chapter XII
Providing classified information in international relations

Section 73
Conditions for providing classified information

Classified information can be provided in international relations unless otherwise stipulated in S. 74

a) classified information at the level TOP SECRET, SECRET, CONFIDENTIAL upon request of the State body, legal person or natural person pursuing business and on the basis of written permission of the Authority;
b) classified information at the level RESTRICTED upon request of the legal person or natural person pursuing business and on the basis of written permission of the central administration office having the subject-matter jurisdiction over classified information; if classified information falls within subject-matter jurisdiction of no central administrative office, on the basis of the written consent of the Authority.

Section 74
Conditions for the provision of classified information between the State body and a foreign power

(1) Fulfilment of the conditions according to S. 73 (a) for providing classified information between the State body and a foreign power will not be required under the following circumstances

a) an international agreement in the area of protection of classified information has been concluded, by which the Czech Republic is bound;
b) providing classified information results from the obligation of the membership of the Czech Republic in the European Union; or
c) classified information is provided in accordance with the special legal regulation[30)].

(2) Classified information at the level RESTRICTED may be provided between the State body and the foreign power without consent laid down in S. 73 (b).

Section 75
Request for permission or approval

(1) If the Applicant is the State body the request according to S. 73 shall contain identification of the foreign power to which classified information should be provided, and if the Applicant is a legal person or natural person pursuing business the request according to S. 73 shall contain identification of the foreign partner and the grounds on which the permission or approval is required.

(2) The agreement between the legal person or natural person pursuing business and their foreign partner containing conditions for protection of classified information to be provided and the list of classified information to be provided shall be appended as an annex to their request for permission or approval according to S. 73.

Section 76
Permission and consent in the process of providing classified information

(1) Prior to the issuance of permission according to S. 73 (a) the Authority shall always require the written opinion of the Ministry of Foreign Affairs and of the Intelligence Service concerned, and further of the central administrative office having the subject-matter jurisdiction over classified information, if the permission is not required by this State body; if classified information falls within the subject-matter jurisdiction of no central administrative office, no opinion will be required. If the permission is required by the legal person or natural person pursuing business the Authority shall request from that person Security Authorization of its foreign partner issued by the authority of the foreign power having the jurisdiction over the protection of classified information in the country of the foreign partner.

(2) The Ministry of Foreign Affairs, the Intelligence Service concerned and the central administrative office shall forward opinions to the Authority according to paragraph 1 within a period of 30 days from the date of delivery of its request.

(3) The Authority will issue the permission (according to) S. 73 (a) within a period of 60 days from the date of delivery of the request of the State body, legal person or natural person pursuing business; the Authority shall not affirmatively dispose of the request if classified information could be endangered by its provision, and the Applicant shall be notified in writing thereof within the above outlined period.

(4) The central administrative office or the Authority will issue the permission according to S. 73 (b) within a period of 30 days from the date of delivery of the request of the legal person or natural person pursuing business; the central administrative office or the Authority shall not affirmatively dispose of the request if classified information could be endangered by its provision and the Applicant shall be notified in writing thereof within the above outlined period.

(5) No legal claim can be laid to the issuance of permission and to the granting of approval according to S. 73.

(6) The Authority shall maintain review of permissions issued according to S. 73 (a).

Section 77
Method of providing classified information

(1) Providing classified information at the security classification levels TOP SECRET, SECRET or CONFIDENTIAL in international relations shall be carried out through the registry as outlined in S. 79 par. 2, unless otherwise stipulated in paragraphs 2 to 5, in S. 78 or in international agreement.

(2) Paragraph 1 shall not apply to providing classified information between the Intelligence Service and similar services of the foreign power

within the frame of co-operation carried out according to the special legal regulation[19)]. The responsible person of the Intelligence Service shall be the authority for deciding on the releasing classified information in these cases.

(3) Paragraph 1 will not apply to providing classified information between the Ministry of Defence, Ministry of Justice, courts, prosecuting attorney's offices, Police or customs bodies and similar bodies of a foreign power, save as otherwise provided in the international agreement by which the Czech Republic is bound, or in the special legal regulation[31)].

(4) State bodies and the Police shall keep records of classified information provided in accordance with paragraphs 2 and 3.

(5) Provisions of paragraph 1 and provisions of S. 73 will not be applied when classified information is to be provided in international relations in the cases according to S. 60 par. 1.

(6) Classified information of a foreign power may be provided to any other foreign power only in accordance with requirements of the releasing foreign power.

Section 78
Method of providing classified information of the European Union within and outside the European Union

(1) Providing classified information at the levels SECRET or CONFIDENTIAL between the Czech Republic and member states of the European Union or between the Czech Republic and bodies of the European Union relating to the mutual co-operation of member states of the European Union according to Treaty on European Union or Treaty establishing the European Community shall be carried out through a registry maintained by the Ministry of Foreign Affairs according to S. 79 par. 3.

(2) The provision of paragraph 1 will not apply to providing classified information requiring a Special Handling Regime according to S. 21 par. 3.

Section 79
Registries of classified information being provided

(1) In registries of classified information TOP SECRET, SECRET or CONFIDENTIAL classified information will be recorded and stored or released, which was provided in international relations.

(2) The Authority shall establish and maintain the central registry of classified information outlined in paragraph 1 that have been directly provided to the Authority or by the Authority and of classified information that are provided through the Authority according to S. 77 par. 1 (hereinafter "the Central Registry").

(3) A State body, legal person and natural person pursuing business shall establish and maintain a registry of classified information outlined in paragraph 1, provided to them or by them (hereinafter "the Registry"); in the Registry of the Ministry of Foreign Affairs also classified information will be maintained that has been provided through the Ministry according to S. 78 par. 1. The Authority upon written request of the State body, legal person or natural person pursuing business shall approve establishment of the Registry; this does not apply to the Intelligence Services. Prior to granting the approval the Authority is authorised to check the particulars in the request for establishment of the Registry, or other facts and conditions specific to the establishment of the Registry, as applicable.

(4) If classified information outlined in paragraph 1 has not been provided by a foreign power or foreign partner of legal person or natural person pursuing business as set out in S. 77 par. 1 or S. 78 par. 1, the State body, legal person or natural person pursuing business shall forward classified information being provided to be recorded immediately after its provision in the Central Registry, or, in the case of classified information according to S. 78 par. 1, in the Registry of the Ministry of Foreign Affairs.

(5) The State body, legal person or natural person pursuing business will report to the Authority changes, which took place in the Registry, to the extent determined by the implementing legal regulation.

(6) The Authority shall maintain records of established registries and carry out checks of their activities.

(7) The implementing legal regulation shall determine

a) organization and activities of the Central Registry;
b) content of written request for establishment of the Registry;
c) conditions for establishment, content and method of management of the Registry; and
d) range of changes in the Registry to be reported to the Authority.

PART THREE
SECURITY ELIGIBILITY

Section 80
Sensitive activities

(1) The sensitive activities mean activities determined by this Act (S. 88) or by the special legal regulation[32)], misuse of which could result in damage to the interest of the Czech Republic.

(2) A natural person who is eligible in terms of security or who is a holder of valid PSC may perform sensitive activities.

(3) Such a person will be eligible in terms of security that is a holder of valid certificate of security eligibility of the natural person (hereinafter "the Certificate").

Section 81
Conditions for issuance of the Certificate

(1) The Authority will issue the Certificate to the natural person who

a) has complete legal capacity;
b) is aged 18 or over;
c) has no criminal record;
d) is personally eligible; and
e) is reliable.

(2) A statement made by the natural person of the legal capacity will prove the condition of legal capacity. The condition of age will be proved by ID card or by travel document of the natural person. The condition that the natural person should not have any criminal record (condition of suitability) will be proved by a statement of criminal records[11)] and, in the case of a foreigner, by a similar document issued by the foreigner's parent nation, as well as by the document of the country, in which the foreigner has resided for at least six consecutive months in the last two years. The document certifying no criminal record shall apply only for three months. The condition of personal eligibility will be verified as outlined in S. 13 par. 2.

Section 82
Suitability
(Condition of no criminal record)

The condition for purposes of security eligibility, that the natural person should have no criminal record, will be satisfied by the natural person who has not been finally and conclusively condemned of an intentional crime, or who is regarded to be a person who had not been condemned.

Section 83
Personal eligibility

The condition of personal eligibility for purposes of security eligibility will be satisfied by the natural person who does not suffer from any disorder or troubles that could affect his/her reliability with respect to performance of sensitive activities.

Section 84
Reliability

(1) The natural person will satisfy the condition of reliability if no adverse circumstance becomes known concerning this person.

(2) The adverse circumstance means activities of the natural person against interests of the Czech Republic.

(3) Also the following can be considered to be the adverse circumstance

a) stating the false information, concealment of material information for unbiased determination of facts of a case in verifying conditions for issuance of the Certificate, or not reporting the change to the data in the application according to S. 99 or in other material provided to the Authority in annex to this application;
b) sentence imposed upon a final and conclusive judgment; or
c) conduct, influential conduct or untrustworthiness of the natural person that could result in misuse of performance of sensitive activities.

(4) Enquires of adverse circumstances as outlined in paragraphs 2 and 3 shall cover the period of 10 years from the date of submitting the

application according to S. 99 or from the age of 15 to the present, whichever is the shorter.

(5) In evaluating whether the circumstance outlined in paragraph 3 constitutes the adverse circumstance, the extent to which it can affect performance of sensitive activities, period of its occurrence, its extent and character, as well as conduct of the natural person concerned in the period outlined in paragraph 4 shall be taken into account.

Section 85
Certificate

(1) The Certificate shall be the legal instrument. The validity of the Certificate shall be five years.

(2) The Certificate shall contain

a) name, surname, maiden name;
b) day, month, year of birth, birthplace;
c) birth registration number (personal identity number);
d) nationality;
e) date of issuance and validity period;
f) official stamp and signature of the authorised representative of the Authority or, if this Certificate was issued in the electronic form, the electronic signature of the authorised representative of the Authority in accordance with the special legal regulation[22)].

(3) Validity of the Certificate shall terminate

a) upon expiry of its validity period;
b) on the date of enforcement of a decision of the Authority (S. 123 par. 3, S. 126 par. 4) to terminate its validity (S. 101);
c) upon the death of the natural person who is a holder of the Certificate or upon declaration of a natural person's death;
d) upon notice of its loss or theft;
e) as a result of the damage to the extent resulting in illegibility of records in the document or causing a breach of its completeness; or
f) upon notice of change to data contained therein.

(4) The performance of sensitive activities will not be affected by the termination of validity of the Certificate according to paragraph 3 (d), (e) and (f); in this case the Authority shall issue, upon written request, within five days from the delivery of the request a new Certificate that replaces the original Certificate.

(5) The format of the Certificate shall be determined by the implementing legal regulation.

Section 86
Obligations of the legal person, natural person pursuing business and of the State body

A legal person, natural person pursuing business and the State body shall

a) ensure that the sensitive activities will be performed by a natural person who is a holder of the valid Certificate;
b) keep records of natural persons who are holders of the valid Certificate and who are in service relationships or in employment relationships, member relationships or similar relationships in respect of them; and
c) report in writing to the Authority circumstances that can affect decisions concerning the issuance or termination (S. 101) of the validity of the Certificate.

Section 87
Obligations of the natural person

(1) The natural person who is a holder of the Certificate shall

a) hand over the Certificate, the validity of which was terminated according to S. 85 par. 3 (b), (e) or (f) to the Authority within five days;
b) report immediately in writing to the Authority the loss or theft of the Certificate;
c) report immediately in writing to the Authority changes to the data in the Certificate; and
d) report immediately in writing to the Authority changes to the data in the application according to S. 99 par. 2 (a), (b) and (d).

(2) Each individual shall forward immediately any Certificate found to the Authority, to the Police or to the Embassy of the Czech Republic.

(3) Each person who made an application according to S. 99 shall report immediately in writing to the Authority changes to the data in the application for the Certificate.

Section 88
Performance of sensitive activities for the needs of the Intelligence Services

(1) Actions of persons not mentioned under S. 140 par. 1 (a) performed for the Intelligence Service

upon agreement, in connection with the performance of the state administration or for other reasons, will be considered to be the sensitive activities for the needs of the Intelligence Service.

(2) The Intelligence Service shall verify conditions of security eligibility of the natural person who should perform sensitive activities for the Intelligence Service.

(3) The Intelligence Service will verify conditions according to S. 81 on its own initiative to the extent necessary for the performance of sensitive activities. A security clearance procedure will not be carried out and no Certificate will be issued.

(4) The Intelligence Service will allow the natural person to perform sensitive activities if he/she satisfies conditions according to S. 81 for the period of time necessary to perform these activities.

PART FOUR
SECURITY CLEARANCE PROCEDURE

Chapter I
Common provisions

Section 89
Common principles of the security clearance procedure

(1) The Authority shall act during the security clearance procedure (hereinafter "the Procedure") in such a way as to ascertain completely and exactly facts of the case to the extent necessary for the decision.

(2) During the Procedure, personal honour and dignity must be protected of all persons involved in the Procedure.

(3) During the Procedure all negotiations shall be conducted and documents made in the Czech language, with the exception of the execution of rights of a member of the national minority according to the special legal regulation[33)]. Documents made in a foreign language shall be presented by participant in the Procedure in original wording together with officially authenticated translations into the Czech language[34)].

(4) The Authority shall create conditions to avoid any damage to or abridgement of rights of the participant in the Procedure for the reason of his/her health handicap.

(5) The Procedure shall be closed.

(6) The participant in the Procedure may authorise a lawyer or another deputy whom he/she chooses to represent him/her in the Procedure. A letter of attorney shall prove the authority for representation. Only one deputy may represent the participant. Representation shall be out of the question in the case of personal acts.

(7) The participant in the Procedure and his/her representative shall have the right to inspect the security file before the issuance of the decision and to make extracts thereof, with the exception of the part of the file (S. 124) containing classified information.

Section 90
Exclusion from the Procedure

(1) Any employee of the Authority directly participating in the Procedure (hereinafter "the Person in Authority") who can be reasonably anticipated to have such interests in the course and results of the Procedure, with respect to his/her relation to the case, to the participant in the Procedure or to his/her representative, for which his/her impartiality can be in doubt, shall be excluded from all acts associated with the Procedure, during which he/she could affect the result of the Procedure.

(2) Also such a Person in Authority shall be excluded who participated in the Procedure in the same case at another level of the Procedure.

(3) The participant in the Procedure may lodge an objection against the prejudice of the Person in Authority within 15 days upon learning of the participation of such a Person in Authority in the Procedure. The objection against the prejudice shall contain, among common formalities, against what Person in Authority the objection is directed, what is considered to be a reason for doubts concerning impartiality of the Person in Authority and what evidence can substantiate his/her allegation. The later submitted objection will not be taken into account.

(4) The Person in Authority who becomes aware of circumstances indicating his/her prejudice shall immediately notify his/her superior officer thereof. Until such time as the superior officer has decided whether he/she shall be excluded, the Person in Authority may perform only such acts that cannot be delayed.

(5) No remonstrance shall be permitted against exclusion of the Person in Authority.

(6) Paragraphs 1 and 3 to 5 will be applied similarly also in the case of participation of experts and interpreters in the Procedure.

Section 91

During the Procedure the Authority shall decide applications according to S. 94, 96 and 99 and termination of validity of the PSC, FSC or of the Certificate according to S. 101.

Section 92
Participant in the Procedure

The following subjects shall be participants in the Procedure

a) in the case of the Procedure concerning applications according to S. 94 or 99 the natural person who requests for issuance of the PSC or Certificate, or the person for whom the issuance of the PSC will be required according to S. 93 par. 1 (b);
b) in the case of the Procedure according to S. 96 the facility that requests for issuance of the FSC;
c) in the case of the Procedure concerning termination of the PSC, FSC or Certificate according to S. 101 the holder of these legal instruments.

Chapter II
Course of the Procedure

Section 93
Initiation of the Procedure

(1) The Procedure will be initiated on the date of

a) delivery of the written application to the Authority according to S. 94, 96 or 99;
b) delivery of the request of the body of the European Union to the Authority for issuance of the PSC – for a national of the Czech Republic who is an employee of a body of the European Union;
c) delivery of the written notice of the Authority to the holder of a PSC, FSC or Certificate of initiation of the procedure concerning termination of validity of these legal instruments (S. 101);
d) delivery of the decision of the director of the Authority on remonstrance (S. 125) issued according to S. 131 par. 3.

(2) In the case of the procedure concerning termination of validity of the PSC or Certificate according to paragraph 1 (c) the Authority shall also notify the responsible person of the holder of these legal instruments of initiation of the procedure.

Application of the natural person
Section 94

(1) An application for issuance of the PSC (hereinafter "the Application of the Natural Person") shall contain written justification of the need of the individual concerned to have access to classified information together with an indication of security classification level that shall be confirmed by the responsible person or by the body that will provide classified information to the natural person.

(2) The following shall be attached to the application according to paragraph 1 by the natural person

a) a completed questionnaire of the natural person in paper and electronic form;
b) originals of documents or verified copies thereof certifying correctness of data stated in the questionnaire that he/she has in hold;
c) a statement of personal eligibility;
d) a statement of legal capacity;
e) one photograph sized 35 x 45 mm corresponding to the present appearance of the natural person, from the front view with the length of head from eyes to chin 13 mm as a minimum, without glasses with dark glass, with the exception of blind individuals, the person shall be dressed in plain clothes and without headgear, if its use is not substantiated by religious or health reasons; in such cases the headgear shall not cover the face in such a way that identification of the natural person would be made impossible.

(3) Appendices according to paragraph 2 shall be considered to be a part of the Application of the Natural Person.

(4) When the natural person should have access to classified information also immediately on the expiry of the validity period of his/her current PSC, he/she shall request in writing the Authority for issuance of the PSC before the expiration of a validity period of the current PSC within the period at least

a) four months in the case of a PSC for the security classification level CONFIDENTIAL;

b) ten months in the case of a PSC for the security classification level SECRET; and
c) thirteen months in the case of a PSC for the security classification level TOP SECRET.

(5) Application according to paragraph 4 shall comply with elements according to paragraph 1 and all appendices according to paragraph 2 shall be attached. Data in the personnel questionnaire shall be completed as described by the implementing legal regulation. Documents according to paragraph 2 (b) will be attached to the application only if during the validity period of the PSC a change occurs to the data that are contained in these documents.

(6) If the natural person according to paragraph 4 requests issuance of the new PSC for the same security classification level, for which he/she has been issued with the current PSC, investigation for determining whether the new PSC can be issued shall be carried out retrospectively, covering at least the period since issuance of the previous PSC.

(7) If a body of the European Union requests issuance of the PSC according to S. 93 par. 1 (b), the natural person concerned shall proceed in accordance with paragraphs 2 to 6 similarly.

Section 95
Personnel Questionnaire

(1) The personnel questionnaire shall contain the following items to be completed:

a) name, surname including all earlier used surnames, and university degrees;
b) date, months, year and place of birth and birth registration number (personal identity number);
c) citizenship status (nationality), present and past;
d) permanent address and address of any other residence where the natural person lives or lived in the last ten years;
e) identity card number and date and place of its issuance, in the case of a foreigner travel document number or similar document number;
f) name of employer and identification of the position being held or identification of activities being executed;
g) names of previous employers including data of formation and termination of employment relationship or service relationship;
h) family status;
i) period of performance of compulsory military service or of alternative service; in the case of a soldier number of military identity card, place of its issuance, military rank achieved, in the case of a civilian reason for termination of liability to military service;
j) business activities;
k) stays abroad exceeding 30 days;
l) orders to execute a judgment;
m) criminal proceedings;
n) previous security clearance procedures;
o) membership of, contacts and associations with former and present security services of a foreign power or with its services in the area of intelligence and with units outlined in S. 14 par. 3 (a);
p) personal contacts not related to employment with non-EU states or non-NATO state nationals, with nationals of the Czech Republic living abroad and with foreign nationals living in the Czech Republic;
q) any narcotics or psychedelic drugs abuse, which are described in the law regulating the area of habit forming substances[35)] and alcohol consumption;
r) pathological gambling;
s) treatment for addiction to substances listed in (q) and to alcohol and treatment for pathological gambling;
t) names and locations of schools after termination of compulsory schooling;
u) property owned;
v) membership of associations, foundations and beneficiary associations within the most recent five years;
w) membership in bodies of legal persons;
x) name of a health insurance company, with which the natural person has medical insurance;
y) delivery address;
z) data according to points (a) to (d) concerning minors; and
aa) data according to points (a) to (d), (f) and (v) concerning spouse and persons aged 18 or over sharing the natural person's living quarters[36)].

(2) Curriculum vitae and statement of truthfulness and completeness of data listed in personnel questionnaire shall be a part of the questionnaire.

(3) Data according to paragraph 1 point (z) will not be completed in the case of an application of a natural person for the security classification level CONFIDENTIAL.

Section 96
Application of the facility

(1) Application of the facility shall contain written justification of the need of the facility

concerned to have access to classified information together with an indication of security classification level and the form of occurrence of classified information.

(2) The facility shall attach the following to the application according to paragraph 1

a) completed questionnaire of the facility in paper and electronic form;
b) security documentation of the facility; and
c) originals of documents or verified copies thereof necessary to verify compliance with conditions according to S. 16.

(3) Appendices according to paragraph 2 shall be considered to be a part of the application of the facility.

(4) When the facility should have access to classified information also immediately on the expiry of the validity period of its FSC, it shall request in writing the Authority for issuance of the new FSC before the expiration of a validity period of current FSC within the period at least

a) four months in the case of FSC for the security classification level RESTRICTED;
b) seven months in the case of FSC for the security classification level CONFIDENTIAL;
c) ten months in the case of FSC for the security classification level SECRET; and
d) thirteen months in the case of FSC for the security classification level TOP SECRET.

(5) The application according to paragraph 4 shall comply with elements according to paragraph 1 and all appendices according to paragraph 2 shall be attached. Only those data in the facility questionnaire shall be completed that have changed during the period of validity of the FSC and that have not been reported to the Authority according to S. 68 (c) and (d). Only those changes will be entered in the security documentation of the facility that have not been reported to the Authority according to S. 68 (d). Documents according to paragraph 2 (c) will be attached to the application only if they are related to changes to the data in the questionnaire that have not been reported to the Authority according to S. 68 (d).

Section 97
Facility Questionnaire

The facility questionnaire shall contain the following items to be completed:

a) data that are entered in the Commercial Register, Register of Trades or similar register or records;
b) name and surname, company and identification number of members of the company if these are not data that is registered in the Commercial Register;
c) names of bank institutions and numbers of bank accounts including accounts closed within the past five years;
d) immovables and non-residential premises of the facility owned and under-lease housing the security area according to S. 25;
e) amount of the net corporate assets of the facility on the date of closing the books of accounts for respective years during the past five years;
f) data from the books of accounts being closed[37)] for the respective years certified by the auditor if determined by the special legal regulation, and data from income-tax returns[38)] for the past five years;
g) loans and credits provided and contracted for the past five years;
h) mortgaged corporeal and real property for the past five years;
i) contracts subject matter of which contains classified information;
j) identification of the tax consultant by the Firm or name, identification number and location in the case of a legal person, in the case of a natural person, by his/her name, surname, birth registration number (personal identity number) and permanent residence;
k) foreign business partners together with total financial volume of trades carried out within the past five years;
l) Czech business partners together with total annual payments of trade carried out and exceeding 20% of turnover within the past five years;
m) name, surname, date of birth and nationality of individuals in employment relationship, member relationship or similar relationship who are not nationals of the Czech Republic;
n) information on filing a bankruptcy petition;
o) information on decision in respect of bankruptcy petition;
p) information on the manner of settlement of bankruptcy;
q) information on dissolution; and
r) performance of obligations in respect of the State according to S. 17 par. 2 (a) and (b).

Section 98
Facility security documents

Facility security documents shall determine the system of protection of classified information at the facility, and shall be updated periodically, and contain the following

a) a listing of classified information held by the facility, indicating its originator and security classification level, and if classified information has been provided to or created by the facility upon order, also the specification of this order shall be indicated, and further the specification of classified information to which the facility should have access, indicating its originator and security classification level, and if classified information should be provided to or created by the facility upon order also the assumed specification of this order shall be indicated;
b) an analysis of possible threat to classified information, suitable and effective protective measures to ensure risks reduction;
c) methods of implementation of individual modes of providing the protection of classified information;
d) a time schedule of implementation of security documents;
e) a list of positions where access to classified information is anticipated and a list of persons who should have access to classified information, indicating their birth registration number (personal identity number) and security classification level required by these persons in their application for issuance of PSC, and in the case of the PSC already issued its number and date of issuance and security classification level for which it was issued.

Application for the Certificate
Section 99

(1) The application for the Certificate shall contain written justification of the performance of sensitive activities confirmed by the responsible person.

(2) The following shall be enclosed in the application according to paragraph 1 by the natural person

a) a completed questionnaire in paper and electronic form;
b) a statement of personal eligibility;
c) original of documents or verified copies thereof certifying the correctness of data stated in the questionnaire;
d) a statement of legal capacity;
e) a statement of criminal records[11)] or, in the case of a foreigner, a similar document issued by the foreigner's parent nation, as well as documents of countries in which the foreigner has resided for at least six consecutive months in the last two years. Documents certifying no criminal record shall apply only for three months; and
f) one photograph sized 35 x 45 mm corresponding to the present appearance of the natural person, from the front view with length of head from eyes to chin 13 mm as a minimum, without glasses with dark glass, with the exception of blind individuals, the person shall be dressed in plain clothes and without headgear, if its use is not substantiated by religious or health reasons; in such cases the headgear shall not cover the face in such a way that identification of the natural person would be made impossible.

(3) Appendices according to paragraph 2 shall be considered to be a part of the application for the Certificate.

(4) When the natural person should perform sensitive activities also immediately on the expiry of the validity period of the Certificate, he/she shall request the Authority for issuance of the new Certificate at least three months before the expiration of the validity period of the current Certificate.

(5) The application according to paragraph 4 shall comply with elements according to paragraph 1 and all appendices according to paragraph 2 shall be attached. Data in the questionnaire shall be completed as described by implementing legal regulation. Documents according to paragraph 2 (c) will be attached to the application only if during the validity period of the Certificate a change occurs to the data that are contained in these documents.

(6) If a natural person requests issuance of a new Certificate according to paragraph 4, the investigation for determining whether the new Certificate can be issued shall be carried out retrospectively, covering at least the period since the previous issuance of the Certificate.

Section 100
Questionnaire

(1) The questionnaire according to S. 99 par. 2 (a) shall contain the following items to be completed

a) name, surname including all earlier used surnames, and university degrees;
b) day, month, year and place of birth and birth registration number (personal identity number);
c) citizenship status, present and past;
d) permanent address and address of any other residence where the natural person lived;
e) identity card number and date and place of its issuance, in the case of a foreigner the travel document number or similar document number;
f) name of employer and identification of the position being held or identification of activities being executed;
g) names of previous employers including data of formation and termination of employment relationships or service relationships;
h) family status;
i) period of performance of compulsory military service or of alternative service; in the case of a soldier the number of his/her military identity card, place of its issuance, military rank achieved, in the case of a civilian the reason for termination of liability to military service;
j) business activities;
k) orders to execute a judgment;
l) criminal proceedings;
m) membership of, contacts and associations with former and present security services of a foreign power or with its services in the area of intelligence and with units outlined in S. 14 par. 3 (a);
n) personal contacts not related to employment with non-EU states or non-NATO states nationals, with nationals of the Czech Republic living abroad and with foreign nationals living in the Czech Republic;
o) any narcotics or psychedelic drugs abuse, which are described in the law regulating the area of habit forming substances[35)] and alcohol consumption;
p) pathological gambling;
q) treatment for addiction to substances listed in point (o) above and to alcohol and treatment for pathological gambling;
r) property owned;
s) name of the health insurance company, with which the natural person has medical insurance;
t) delivery address.

(2) The curriculum vitae and statement of truthfulness and completeness of data listed in this questionnaire shall be the part of the questionnaire.

Termination of validity of the personnel security clearance, facility security clearance or of the Certificate
Section 101

(1) The Authority shall initiate the procedure directed to termination of the PSC, FSC or Certificate if there is a reasonable doubt whether the holder of such legal instrument continues to meet conditions for its issuance (S. 12, 16 and 81).

(2) If a holder of the PSC, FSC or of the Certificate no longer meets conditions for issuance of such legal instrument, the Authority will terminate its validity.

Common provisions
Section 102

(1) If the Application of the Natural Person, application for Certificate or application of the facility has not complied with required elements, the Authority will afford assistance to the participant in the procedure in elimination of these formal defects. If these defects cannot be corrected on the spot, the Authority shall immediately request the participant in the Procedure to correct these defects within 30 days of the service of the request; briefing on consequences shall be part of the request, if the data necessary for continuing the Procedure are not completed in time [S. 113 par. 1 (c)].

(2) At the request of the participant in the Procedure the Authority will acknowledge acceptance of the application of a natural person, application for the Certificate or application of the facility,.

Section 103

(1) If necessary for complete and truthful facts finding, the Authority is entitled to request specification of data listed in the application according to S. 94, 96 and 99 from the participant in the Procedure. For this purpose the Authority will request in writing the participant in the Procedure to submit this specification to the Authority within 14 days of the service of the request.

(2) During the Procedure the participant in the Procedure shall immediately notify in writing the Authority of any changes to the data listed in the application according to S. 94, 96 and 99.

Section 104
Witness

(1) Each individual shall testify as a witness for the purpose of finding the facts of a case and determination of possible security risks, and attend as a witness on summons at the Authority. It must be clear from the summons, when, where and in what case the witness shall attend and what are the consequences in law arising from the fact of non-attendance (S.115, S.116). The witness shall testify truthfully and completely. Any individual shall not be examined as a witness, who would breach the protection of classified information or the duty to maintain confidentiality imposed or recognized by the law, unless he/she has been released from this duty. The witness can refuse to give the testimony only if it could put him/her or an immediate family member at risk of criminal prosecution[39)]. The testimony may also be refused by the person who has close ties of affection to a participant in the Procedure.

(2) The Authority shall establish the identity of a witness and brief him/her according to paragraph 1 and on the legal consequences of untrue or incomplete testimony (S. 116).

(3) A report on witness testimony shall be made. S. 105 par. 5 and 6 shall apply by analogy concerning making the report on a witness testimony.

(4) The Authority shall reimburse proved cash expenses to the witness and loss of earnings in accordance with the law regulating travelling expenses[40)]. A claim shall be filed within five days from the witness testimony otherwise it will expire. The witness shall be warned in advance thereof.

(5) Any Police officer or member of the Intelligence Service who participates in the Procedure shall not be examined as a witness.

(6) Acts in the Procedure according to S. 107 to 109 shall not be replaced by the witness testimony.

Section 105
Security interview

(1) When information comes to light that should be inquired in order to find the facts of the case, the Authority shall ensure that the participant in the Procedure will be interviewed; in the case of a participant in the Procedure who requests a PSC for the level TOP SECRET the security interview by the Authority shall be conducted in all cases.

(2) The participant in the Procedure shall be summoned to the security interview in writing. It must be clear from the summons, when, where and in what case and for what reason the participant in the Procedure shall attend and what are the consequences in law arising from the fact of non-attendance [S. 113 par. 1 (d)].

(3) During the course of a security interview the participant in the Procedure shall provide requisite information personally; no lawyer or other proxy is entitled to intervene in the course of the interview.

(4) Prior to commencement of the security interview each participant in the Procedure shall be briefed in writing on the importance and purpose of the interview and on possible consequences in the case of a false or incomplete statement [(S. 113 par. 1 (h)].

(5) A report on the security interview shall be made. The report shall contain the place, time and subject matter of the interview, as well as data permitting identification of the participant in the Procedure, Person in Authority and of other individuals participating in the interview.

(6) The report shall be signed by the participant in the Procedure, Person in Authority or recorder or interpreter; signature of the participant in the Procedure shall be on each page of the record. Refusal to sign the record and reasons for this refusal shall be entered in the record. The security interview may be recorded on audio or video media only with consent of the participant in the Procedure; the record shall be made whenever requested by the participant in the Procedure. This record shall be the part of the security file (S. 124).

(7) No classified information shall be disclosed during the course of a security interview.

(8) A security interview with a participant in the Procedure with long-term residence abroad may be substituted by his/her written statement. The Authority shall communicate all information to this individual that should be the subject of the statement. The signature of the participant in the Procedure shall be on each page of the written statement.

Section 106
Expert

(1) If, during investigation of condition of personal eligibility in the cases according to S. 13 and 83, facts are revealed by the Person in Authority giving rise to doubts as to the personal eligibility of the participant in the Procedure, the Authority will appoint an expert[41)] for making an expert's report on personal eligibility.

(2) If the expert's report is needed for expert evaluation of facts important for the final decision and if these facts are not as outlined in paragraph 1, the Authority will appoint the expert[41)].

(3) The costs of making an expert's report according to paragraph 1 and 2 will be reimbursed by the Authority

Acts during the course of the Procedure
Section 107
Acts during the course of Procedure for granting the personnel security clearance

(1) During the course of the Procedure for granting the PSC for the security classification level CONFIDENTIAL, the Authority will require the necessary information from the competent State body, legal person or natural person pursuing business, provided they handle such information, for verification truthfulness of data given by the participant in the Procedure in the natural person application, and for determination of occurrence of security risks.

(2) During the course of the Procedure for granting the PSC for the security classification level SECRET, the Authority shall proceed in accordance with paragraph 1, and further verify the identity of the participant in the Procedure; concerning verification of identity of the participant in the Procedure it may contact the Intelligence Service concerned or the Police, as necessary. If information obtained is not sufficient for full determination of facts of the case, it can be verified or completed upon the request of the Authority by investigation of the Intelligence Service concerned or the Police with respect to the participant in the Procedure and with respect to individuals aged 18 or over living in a common household[36)].

(3) During the course of the Procedure for granting the PSC for the security classification level TOP SECRET, the Authority shall proceed in accordance with paragraph 2, and further ask the Intelligence Service concerned for investigation of security risks in the background of the participant in the Procedure.

(4) The Intelligence Services and the Police shall comply with the request of the Authority according to paragraphs 2 and 3 and submit report on results of investigations being requested.

(5) If information obtained during the course of the Procedure for granting the PSC for the security classification level CONFIDENTIAL is not sufficient for full determination of facts of the case, the Authority shall be entitled to verify it by acts according to paragraphs 2 and 3, and during the course of the Procedure for granting the PSC for the security classification level SECRET according to paragraph 3. In these cases the Authority shall request written consent of the participant in the Procedure and brief him/her at the same time on legal consequences if the Authority does not receive the written consent [S. 113 par. 1 (e)].

(6) If the Procedure is conducted upon application according to S. 94 par. 4, the Authority shall be entitled to perform acts according to paragraphs 1 to 5. Provisions of the paragraph 5 of the second sentence shall apply by analogy.

Section 108
Acts during the course of the Procedure for granting the facility security clearance

(1) During the course of the Procedure for granting the FSC for the security classification level RESTRICTED, the Authority will verify truthfulness of data given by the participant in the Procedure in the facility application for determination of economic stability, security suitability and for verification of capability of the facility to maintain protection of classified information; for this purpose the Authority will require the necessary information from the competent State body, legal person or natural person pursuing business, provided they handle such information.

(2) During the course of the Procedure for granting the FSC for the security classification level CONFIDENTIAL, the Authority shall proceed in accordance with paragraph 1, and further verify ownership relations at the facility. If the Authority cannot verify ownership relations at the facility, the Authority can ask the competent Intelligence Service or the Police for this verification.

(3) During the course of the Procedure for granting the FSC for the security classification level

SECRET, the Authority shall proceed in accordance with paragraph 2, and further verify commercial relations of the facility. If the Authority cannot verify commercial relations of the facility, the Authority can ask a competent Intelligence Service or the Police for this verification.

(4) During the course of the Procedure for granting the FSC for the security classification level TOP SECRET, the Authority shall proceed in accordance with paragraph 3 and further perform other acts for verification of significant capital and financial relations of the facility. If the Authority cannot verify capital and financial relations of the facility, the Authority can ask competent Intelligence Service or the Police for this verification.

(5) The Intelligence Services and the Police shall comply with the request of the Authority according to paragraphs 2 and 4 and submit a report on the results of investigations being requested.

(6) If information obtained during the course of the Procedure for granting the FSC for the security classification level RESTRICTED is not sufficient for full determination of facts of the case, the Authority shall be entitled to verify it by acts according to paragraphs 2 to 4, during the course of the Procedure for granting the FSC for the security classification level CONFIDENTIAL according to paragraphs 3 and 4, and during the course of the Procedure for granting the FSC for the security classification level SECRET according to paragraph 4. In these cases the Authority shall request written consent of the participant in the Procedure and brief him at the same time on the legal consequences if the Authority does not receive the written consent [S. 113 par. 1 (e)].

(7) If the Procedure is conducted upon application according to S. 96 par. 4, the Authority shall be entitled to perform acts according to paragraphs 1 to 6. Provisions of paragraph 6 of the second sentence shall apply by analogy.

Section 109
Acts during the course of Procedure for granting the Certificate

(1) During the course of Procedure for granting the Certificate the Authority will require the necessary information from the competent State body, legal person or natural person pursuing business, provided they handle such information.

(2) If information obtained according to paragraph 1 is not sufficient for full determination of facts of the case, it can be verified or completed by other necessary acts according to S. 107, appropriate to the purpose of the Procedure; in these cases the Authority shall request written consent from the participant in the Procedure and brief him on legal consequences if the Authority does not receive the written consent [S. 113 par. 1 (e)].

(3) If the Procedure is conducted upon application according to S. 99 par. 4, the Authority shall be entitled to perform acts according to paragraphs 1 and 2. Provisions of the paragraph 2 of the part of the sentence after the semicolon shall apply by analogy.

Section 110

(1) Within the period of validity of the PSC, Certificate or FSC, prior to issuance of the PSC for a foreign power or the FSC for a foreign power according to S. 57, the Authority shall verify by acts of the Procedure whether the natural person or facility continues to fulfil conditions for the issuance of the PSC, Certificate or FSC.

(2) Upon request of the security authority of the member state of the North Atlantic Treaty Organization, European Union or another state, with which the Czech Republic has concluded the international agreement, having jurisdiction over the protection of classified information, the Authority will perform acts of the Procedure concerning a person who is being security cleared in the state concerned for access to classified information.

Section 111

In performing acts according to S. 107 and 108, S. 109 par. 1 and S. 110 the Authority shall be entitled to provide to the State body, legal person or to the natural person pursuing business the requisite personal data relating to the information being requested to the extent necessary.

Section 112
Suspension of the Procedure

(1) The Authority shall suspend the Procedure by its decision if

a) the procedure takes place at another State body that tackles the questions significant for issuance of a decision according to this Act;
b) the participant in the Procedure has been invited by the Authority to remove shortcomings of the natural person application, facility application,

Certificate application or of the remonstrance, or to supplement other data required by the Authority;

c) the participant in the Procedure represented by more responsible persons, but not in conformity, has been invited by the Authority to reach conformity within a prescribed period, or to delegate the negotiation of the subject matter on only one responsible person;
d) the witness cannot be examined whose statement is important for determination of facts of the case;
e) the participant in the Procedure asks for suspension by reason of long-term impediment to participation in the Procedure but for no longer than 60 days; or
f) the expert has been appointed to make the expert's report.

(2) No remonstrance shall lie against the decision to suspend the Procedure.

(3) The Authority shall proceed with the Procedure on its own initiative or on the initiative of the participant in the Procedure, as soon as the obstacle of suspension ceased to exist or the term set out in paragraph 1 (e) expired. The Authority shall notify the participant in the Procedure in writing thereof.

(4) During suspension of the Procedure the terms according to S. 117 and S. 131 par. 6 do not run.

Section 113
Termination of the Procedure

(1) The Authority shall terminate the Procedure by its decision if

a) the participant in the Procedure withdraws the natural person application, facility application, Certificate application or remonstrance (S. 125);
b) the participant in the Procedure does not meet conditions laid down in S. 6 par. 2 or S. 81 par. 1 (a), (b) or (c);
c) the participant in the Procedure has not removed shortcomings within a prescribed period, in the natural person application, facility application, Certificate application or remonstrance (S. 125);
d) the participant in the Procedure did not attend repeatedly in the interview without just excuse containing substantial reasons;
e) the participant in the Procedure did not give his consent according to S. 107 par. 5, S. 108 par. 6 or S. 109 par. 2;
f) the participant in the Procedure did not reach conformity in negotiations of responsible persons within a prescribed period or did not delegate only one responsible person to the negotiation;
g) complete and correct facts of the case cannot be determined because the participant in the Procedure lives or has lived in a foreign country on a long-term basis;
h) the participant in the Procedure has submitted false or incomplete information or does not cooperate to the extent necessary and the case cannot be decided on the basis of the given facts of the case;
i) the participant in the Procedure died or has been declared dead or it was dissolved; or
j) the reason for the procedure initiated according to S. 93 par. 1 (c) disappeared.

(2) The Intelligence Services and the Ministry of the Interior will also terminate the Procedure by decision if the reason of Procedure according to S. 140 par. 1 (a) and S. 141 par. 1 disappears by virtue of incompetence of these State bodies and the Application of the Natural Person has not been withdrawn.

(3) The provision of paragraph 1 (j) will not apply for termination of remonstrance proceedings (S. 131 par. 1) brought against the decision to terminate validity of the PSC, FSC or Certificate.

(4) No remonstrance shall be permitted against the decision to terminate the Procedure according to paragraph 1 (a), (b), (e), (f), (g), (i) and (j) and according to paragraph 2.

Securing of the purpose and course of the Procedure
Section 114
Summons

(1) The Authority shall summon in writing individuals whose participation in hearing the case is necessary.

(2) In summons the Authority shall notify individuals laid down in paragraph 1 of legal consequences of non-attendance.

Section 115
Bringing before the Authority

(1) The witness, who did not attend without just excuse or without substantial reasons at the Authority and without whose personal participation the Procedure cannot be carried out, may be brought before the Authority.

(2) The Authority will ask the Police to bring the witness, in the case of soldiers in active service or members of armed forces their superiors.

Section 116

Procedural fine

(1) The Authority may impose a procedural fine as follows

a) any individual may be fined up to 50,000 CZK who obstructs the course of the Procedure, in particular due to non-attendance without substantial reasons at the Authority on its written notice, gives false or incomplete testimony or refuses to give testimony without reason or to submit the document;
b) any State body, legal person or natural person pursuing business may be fined up to 500,000 CZK if it or he/she does not provide free of charge the Authority with requested information needed for the security Procedure according to S. 117 par. 7.

(2) The fine according to paragraph 1 can be imposed repeatedly. The collective sum of imposed procedural fines shall not exceed the amount of 100,000 CZK in the case of a fine according to paragraph 1 (a), and the amount of 1,000,000 CZK in the case of a fine according to paragraph 1 (b).

(3) S. 156 par. 3 and 7 to 9 will be applied for the determination of the rate of the fine and for determination of its maturity, and for collection and for enforcing the payment of a fine being imposed.

Terms, calculation of time and delivery
Section 117

(1) The Authority shall terminate the PSC Procedure within the following period starting from the date of its initiation

a) three months for the security classification level CONFIDENTIAL;
b) nine months for the security classification level SECRET;
c) twelve months for the security classification level TOP SECRET.

(2) The Authority shall terminate the FSC Procedure within the following period starting from the date of its initiation

a) three months for the security classification level RESTRICTED;
b) six months for the security classification level CONFIDENTIAL;
c) nine months for the security classification level SECRET;
d) twelve months for the security classification level TOP SECRET;

(3) The Authority shall terminate the Certificate Procedure within three months starting from the date of its initiation.

(4) The Intelligence Service concerned and the Police shall forward to the Authority findings of investigation carried out according to S. 107 par. 2, second sentence, and S. 107 par. 3 within the following period starting from the date of delivery of its request

a) six months for the security classification level SECRET;
b) nine months for the security classification level TOP SECRET.

(5) The Intelligence Service concerned and the Police shall forward to the Authority findings of investigation carried out according to S. 108 par. 2 to 4 within the following period starting from the date of delivery of its request

a) three months for the security classification level CONFIDENTIAL;
b) six months for the security classification level SECRET;
c) nine months for the security classification level TOP SECRET.

(6) The Intelligence Service concerned and the Police shall forward to the Authority findings of investigations carried out according to S. 109 par. 2 within two months starting from the date of delivery of its request.

(7) The State body, legal person and the natural person pursuing business shall meet the request of the Authority according to S. 107, 108 or 109 free of

charge within 30 days starting from the date of delivery of the request to provide information.

Section 118

(1) If the Intelligence Service or the Police cannot notify the Authority of the results of an investigation within the periods according to S. 117 par. 4 to 6 it shall inform the Authority thereof.

(2) If the State body, legal person or natural person pursuing business cannot provide information within a period as outlined in S. 117 par. 7 it shall inform the Authority thereof.

(3) If the Authority cannot make a decision due to notification according to paragraph 1 or 2 in terms according to S. 117 par. 1 to 3, the director of the Authority will adequately extend the period and the participant in the Procedure shall be notified by the Authority in writing thereof together with reasons for the delay.

(4) An extension of time according to paragraph 3 may never be longer than the timeframe required for carrying out the Procedure for the corresponding level.

Section 119
Calculation of time

(1) The day on which the circumstance determining the beginning of the term occurred will not be included into the term. Terms determined according to months or years will expire on the date that conforms by its marking with the date when the circumstances determining the beginning of the term occurred, if there is no such date in the month, the term will end on the last day of the month. If the final date of the term falls on a weekend or holiday the next working day will be the last date of the term.

(2) The term will be observed if submission is made with the Authority at least on the last day of the term or if the mail addressed to the Authority has been posted on that day, which contains submission, to the postal licence holder or to the special postal licence holder[17)] or to a person holding the similar position in another state.

(3) In the case of doubts the term shall be considered to be observed if the contrary is not proved.

(4) When compelling reasons are present and the participant in the Procedure fails to observe the term, the Authority will waive the lapse of time if the participant in the Procedure applies for an extension of time within five days starting from the date when reasons of such a default cease to exist, and if the participant in the Procedure takes action in default within the same timeframe. The Authority may award suspensory effect to this request.

(5) No remonstrance shall be permitted against the motion to waive the lapse of time.

Section 120
Delivery

(1) Decisions and other documents (hereinafter "the Instruments") will be delivered by the Authority itself or through the postal licence holder or special postal licence holder[17)]. Delivery to foreign countries shall take place through the Ministry of Foreign Affairs, save as otherwise provided in the international agreement to which the Czech Republic is bound. All Instruments shall be delivered into the own hands of the recipient.

(2) If the addressee refuses to receive the service of the Instrument, the postal licence holder or the special postal licence holder will mark this on the advice of delivery together with the date, and send the Instrument back to the Authority. The Instrument will be considered given as of the date of refusal of reception of the service of the Instrument; if the delivery takes place by the Authority, the refusal of reception of the service of Instrument will be marked by it similarly.

(3) If the addressee has not been available at the place of delivery, although he/she resides at the place of delivery, the deliverer will deposit the mail with the Authority or in the premises of the postal licence holder or special postal licence holder having local competence. The mail will be deposited for 10 days. The addressee shall be called on by inserting the notice into his letterbox or by another practicable manner to take the delivery. If the addressee does not take the Instrument within 10 days from the date of its deposit, the last day of this period shall be considered as the date of delivery, even if the notification of delivery of the document did not come to the knowledge of the addressee.

(4) If the contrary is not proved, it shall be taken that the addressee has stayed in the place of delivery.

(5) In the case of the natural person the place of delivery shall be the home address in the territory of the Czech Republic indicated by that person. If the

natural person stays abroad on a long-term basis in the interest of the State, the home address in the foreign country may also be the place of delivery.

(6) If the Instrument is delivered to the addressee in a foreign country, the terms according to this Act do not run during the time of delivery.

(7) The Instrument may be delivered to the natural person anywhere he/she will be found. If the addressee refuses to receive the service of the Instrument, the procedure shall apply according to subparagraph 2 accordingly.

(8) In the case of a legal person the Instrument shall be delivered to the address of its location, and in the case of a natural person pursuing business the Instrument shall be delivered to the address of his/her place of business activity. A responsible person or authorised employees are entitled to take delivery of the Instrument on behalf of the legal person.

Decision
Section 121

(1) If the Authority affirmatively disposes of the natural person's application, legal person application or Certificate application it will not issue the written decision. In these cases the Authority will issue the PSC, FSC or Certificate and deliver it to the participant in the Procedure; the Authority will place the copies into the security file (S. 124).

(2) If the Authority does not affirmatively dispose of the natural person application, legal person application or Certificate application it will issue the decision of non-issuance of the PSC, FSC or Certificate and deliver it to the participant in the Procedure; the Authority will place the copy into the security file.

(3) If the Authority terminates validity of the PSC, FSC or Certificate it will issue a decision thereof and deliver it to the participant in the Procedure; the Authority will place the copy into the security file.

(4) In the case of Procedure carried out upon request by the appropriate body of the European Union according to S. 93 par. 1 (b) the Authority will send to this body the notice of results of this Procedure.

Section 122
Elements of the decision

(1) The decision shall be issued in writing and it shall contain statements of the decision, reasoning and briefing of the participant in the Procedure. The Authority shall notify immediately the responsible person of this participant of the coming into force of the decision delivered to the participant in the Procedure, who is the natural person. In the case of termination of validity of the Certificate that has been issued for military material trading according to the special legal regulation[32)] the Authority shall notify the coming into force of the decision to the Ministry of Industry and Commerce.

(2) The solution of the matter that is the subject matter of the decision-making process and provisions of this Act, under which the decision was taken, shall be given in the statements of the decision. The part of the statements of the decision shall also contain a marking of the participant in the Procedure that enables his/her/its identification. If the participant in the Procedure is the natural person, it will be identified by the name, surname and by the birth registration number (personal identity number). If the participant in the Procedure is the facility, it shall be identified by the Firm or the name, company registration number and by its location. The part of statements of the decision may also contain determination of the time limit to perform imposed duty.

(3) Reasons for issuance of the decision shall be provided for in the reasoning, grounds for its issuance, considerations that has been followed by the Authority in their evaluation and in application of legal regulations. If some of the reasons for issuance of the decision is classified information, then only reference to grounds for issuance of the decision and its classification level may be quoted. Considerations that have been followed by the Authority in their evaluation and reasons for issuance of the decision will be quoted only to the extent in which they are not classified information.

(4) It shall be stated in the briefing whether remonstrance may be lodged against the decision, within what time-limit, from what date this time-limit will be calculated, who decides on the remonstrance, with what body it will be lodged, as well as the fact that the remonstrance has no suspensive effect.

(5) Further the decision shall contain identification of the Authority, date of its making, official stamp, name, surname, position and signature

of the employee of the Authority who issued the decision.

(6) The Authority will make correction of evident incorrectness in the written decision anytime even without the motion and the participant in the Procedure shall be notified thereof. If the correction concerns statements of the decision, the Authority shall issue an amended decision thereof. The remonstrance may be permitted against the amended decision.

Section 123
Legal force and enforcement of the decision

(1) The decision shall become effective if it was delivered and no remonstrance may be permitted against it.

(2) The Authority will mark on the decision upon request of the participant in the Procedure, when the decision has become effective.

(3) The decision shall be enforceable if it has become effective or if it has been delivered and the remonstrance against it has no suspensive effect.

Section 124
Security file

(1) The security file contains materials relating to the Procedure and reporting of changes; and it has a classified and unclassified part.

(2) The security file shall be filed, maintained, updated, recorded and discarded by the Authority; it will be discarded after the expiration of 20 years from the date of the last effective decision in the Procedure.

(3) The data in the security file may be used only for the needs of fulfilment of duties according to this Act.

(4) Employees of the Authority who carry out the Procedure shall keep confidential the data entered in the security file that came to their knowledge during carrying out this Procedure or in connection with it.

(5) Upon request by investigative, prosecuting and adjudicating bodies the director of the Authority may relieve individuals outlined in paragraph 4 from obligations to maintain confidentiality.

Chapter III
Remonstrance and judicial review

Basic provisions, terms for lodging the remonstrance and its elements
Section 125

The participant in the Procedure shall have the right to lodge the remonstrance against the decision of the Authority issued in the Procedure, unless he/she/it has waived this right in writing or unless otherwise provided herein.

Section 126

(1) The remonstrance will be lodged with the Authority within 15 days from the date of delivery of the decision.

(2) In the case of missing, incomplete or mistaken briefing the remonstrance may be lodged within three months from the date of delivery of the decision.

(3) The Authority will waive the lapse of time for lodging the remonstrance when compelling reasons are present and when the participant in the Procedure makes request within 15 days starting from the date when reasons of such default cease to exist and the remonstrance has been lodged simultaneously.

(4) Lodging of the remonstrance against the decision to terminate the validity of the PSC, FSC or Certificate has no suspensive effect.

(5) If the participant in the Procedure has withdrawn the remonstrance in writing after expiry of the term according to paragraph 1, he/she/it cannot lodge it again.

Section 127

(1) The remonstrance lodged by the natural person shall contain his/her name, surname, birth registration number (personal identity number) and address of permanent residence or delivery address; it shall be dated and signed.

(2) The remonstrance lodged by the facility shall contain its identification by the Firm or name and identification number, and the address of its location or another delivery address. The remonstrance shall be dated and signed by a person or persons who are authorised to act for the facility.

(3) It shall be further stated in the remonstrance against what decision it is aimed, what the participant in the Procedure seeks and what is considered to be contrary to legal regulations, or other incorrectness of the contested decision. The remonstrance may not be lodged only against the reasoning of the decision.

(4) If the remonstrance has not the requested elements, the Authority shall request the subject that lodged the remonstrance to eliminate deficiencies. It shall determine the time limit in its request for elimination of deficiencies that may not extend beyond 15 days and brief him/her/it of legal consequences if these deficiencies are not eliminated [S. 113 par. 1 (c)].

Practice of the Authority before the decision of the director of the Authority
Section 128

(1) The Authority will dismiss the remonstrance by its decision, without signing its decision by the director of the Authority, if

a) the remonstrance cannot be lodged according to this Act; or
b) the remonstrance has been lodged after the term determined according to S. 126 par. 1, and the default of time for its lodging has been waived according to S. 126 par. 3.

(2) The remonstrance may be permitted against the decision provided for in paragraph 1.

Section 129

(1) The Authority may decide the remonstrance itself, without signing its decision by the director of the Authority, if it allows the remonstrance completely; if the Authority allows the remonstrance, it will cancel the contested decision.

(2) The remonstrance may be permitted against the decision provided for in paragraph 1.

(3) If the Authority does not decide the remonstrance according to paragraph 1 or according to S. 128, it will forward it with its opinion and with all documents, within 15 days from the date of delivery of the remonstrance, to the director of the Authority.

Decision of the director of the Authority in the procedure to deal with the remonstrance
Section 130

(1) The remonstrance will be decided by the director of the Authority upon a motion of the remonstrance commission, if the procedure according to S. 128 par. 1 or S. 129 par. 1 is not applied.

(2) Members of the remonstrance commission shall be appointed and removed by the director of the Authority. The remonstrance commission shall have at least five members. More then half of the members of the commission shall have a university legal education. The members of the remonstrance commission shall be holders of a valid PSC for the security classification level TOP SECRET and nationals of the Czech Republic. The remonstrance commission shall always be established for a period of five years; the chairman of the remonstrance commission shall always be one of the members of this commission for a period of one calendar year. The remonstrance commission is able to act if more than a half of its members are present; the resolution will be adopted by more than half of votes of its members being present.

(3) The majority of members of the remonstrance commission shall be employees of the State assigned in other State bodies than in the Authority; it does not apply to the structure of the commission in the procedure according to S. 140 par. 1 (a).

(4) The membership in the remonstrance commission shall be terminated

a) upon expiration of the term of office of this commission;
b) upon discharge from the position;
c) upon resignation;
d) upon death or declaration of death of a person.

(5) The member of the remonstrance commission is not entitled to the remuneration. The Authority can reimburse travelling expenses in accordance with the Act regulating travelling reimbursements[40)].

Section 131

(1) The director of the Authority shall terminate the procedure to deal with the remonstrance if grounds exist according to S. 113, and cancel the contested decision if the decision has become faint

due to the termination of the procedure; or else it will confirm the contested decision.

(2) The director of the Authority will cancel the contested decision if he/she allows completely the remonstrance lodged against the decision to terminate validity of the PSC, FSC or Certificate.

(3) The director of the Authority shall cancel the contested decision and refer the case back to the new consideration and decision if

a) a contested decision has been issued contrary to legal regulations or is erroneous in another way; or
b) it has been determined that circumstances had arisen after the issuance of the decision that have a bearing on the decision.

(4) The remonstrance shall be dismissed and the decision confirmed by the director of the Authority if he/she does not find any reason for measures according to paragraphs 1 to 3.

(5) In the reasoning of the decision on the remonstrance according to paragraph 3 the director of the Authority shall also deliver a legal opinion by which the Authority shall be bound in the new consideration of the case, unless this legal opinion becomes faint due to a change to the legal status or factual circumstances. In the new Procedure the Authority may use grounds of the original decision including grounds of the decision on remonstrance, unless it is contrary to the grounds for the new Procedure. The remonstrance may be permitted against the decision issued in the new Procedure, unless otherwise provided herein.

(6) The director of the Authority shall decide the remonstrance within three months from the date of delivery of the remonstrance.

Section 132

Validity of the PSC, FSC or Certificate will be renewed as of the date of legal effect of the decision on remonstrance according to S. 129 par. 1 or S. 131 par. 2 or 3, which has been terminated as a result of the contested decision. Together with the decision on remonstrance the PSC, FSC or Certificate will be sent back to the participant in the Procedure that has been forwarded according to S. 66 par. 1 (b), S. 68 (a) or S. 87 par. 1 (a); the validity period of the security clearance or Certificate shall be maintained.

Chapter IV
Judicial review and final provision

Section 133

(1) An action can be brought against the decision of the director of the Authority according to the special legal regulation[42)] within 30 days of the service of the decision. Where the decision of the director of the Authority according to S. 131 par. 1 is in question, the action can be brought only if remonstrance is allowed to be lodged against the grounds to terminate the Procedure according to S. 113 par. 4.

(2) Evidence at the judicial proceedings shall be adduced in such a way so as not to affect the duty to maintain confidentiality concerning classified information contained in results of the investigation or in the data from records of the Intelligence Services or the Police. Evidence by examination concerning these factors may be produced only if the person who has an obligation to maintain confidentiality has been released from that obligation by the appropriate authority; the release from the obligation to maintain confidentiality is not possible only in the cases when threat could arise that may endanger or seriously affect activities of the Intelligence Services or the Police; a similar procedure will be followed also in the cases where evidence is not produced by examination.

(3) The Authority shall mark factors set out in paragraph 2 in respect to these it claims that nobody can be released from the obligation to maintain confidentiality, and the judge presiding over the case shall decide that parts of the file to which these factors apply, will be separated if the activities of the Intelligence Services or of the Police could be endangered or seriously affected; separated parts of the file cannot be inspected by the participant in the Procedure, by his/her representative as well as by the person participating in the Procedure. Provisions of the special legal regulation[42)] relating to the evidence, marking of parts of the file and its inspection shall be without prejudice to any other rights than those limited above.

Section 134

Save as otherwise provided for in paragraphs 125 to 132, appropriate provisions of paragraphs 89 to 124 shall be used accordingly for the procedure to deal with the remonstrance.

Chapter V
Delegating provisions

Section 135

The implementing legal regulation shall determine

a) the format of briefing according to S. 58 par. 5;
b) the formats and way of making applications according to S. 93 par. 1 (a);
c) the list of documents according to S. 94 par. 2 (b);
d) the extent of data of the personal questionnaire in the case of an application according to S. 94 par. 5 and questionnaire in the case of an application according to S. 99 par. 5;
e) the format of the statement of personnel eligibility;
f) the format of the personal questionnaire according to S. 95;
g) the list of documents according to S. 96 par. 2 (c) and their elements and format of the facility questionnaire according to S. 97; and
h) the list of documents according to S. 99 par. 2 (c) and the format of the questionnaire according to S. 100.

PART FIVE
EXECUTION OF THE STATE ADMINISTRATION

Section 136

(1) The state administration in the areas of protection of classified information and security eligibility shall be executed by the Authority, save as otherwise provided herein.

(2) The Authority is headed by the director who shall be appointed by the government, after consideration in the committee of the Chamber of Deputies in charge of the security matters, and the government shall also remove the director from the office

(3) The director of the Authority shall be answerable to the Prime Minister or to the authorised member of the government.

Section 137
The Authority

The Authority as the central administrative authority shall

a) decide the natural person application, facility application and Certificate application, as well as termination of validity of the PSC, FSC and Certificate, with the exception of cases set out herein [S. 140 par. 1 (a) and S. 141 par. 1], and issue personnel security clearances according to S. 56 (a);
b) carry out the state supervision in the areas of protection of classified information and security eligibility (S. 143) and methodical activities, with the exception of cases set out herein (S. 143 par. 5);
c) ensure that specialist competence exams will be made and issue a Specialist Competence Certificate;
d) fulfil tasks in the area of protection of classified information in accordance with obligations due to membership of the Czech Republic in the European Union, North Atlantic Treaty Organization and due to international agreements to which the Czech Republic is bound;
e) maintain the Central Registry and approve establishment of registries in the State bodies and in facilities;
f) permit providing classified information in determined cases internationally;
g) issue courier certificates upon written request of the responsible person for the purposes of courier transportation of classified information to be transported internationally, with the exception of classified information provided according to S. 78 par. 1, and arrange for its transportation in justified cases;
h) ensure activities of the National Communication Security Agency, National Cryptographic material Distribution Agency, National Compromising Electromagnetic Emissions Measurement Agency and National Information Systems Security Agency, which are its parts;
i) carry out a certification of technical means, Information System, cryptographic equipment, cryptographic site and shielded chamber;
j) ensure research, development and production of national cryptographic equipment;
k) develop and approve national cipher algorithms and create national cryptographic protection policy;
l) examine compromising electromagnetic emissions where classified information is or will be stored or handled;

m) examine in co-ordination with the Intelligence Services and with the Police those areas where meetings are held to ensure that no threats to classified information arise and no leakage of classified information takes place as a result of unauthorised use of technical means intended for obtaining information;
n) issue the security standards;
o) impose sanctions for breach of duties as described herein;
p) decide other subject-matters and fulfil other tasks in the areas of protection of classified information and security eligibility as described herein;
q) issue the Bulletin of the Authority publishing the list of certified technical means and the list of the State bodies and facilities, with which the Authority has concluded agreements according to S. 52. The content of the Bulletin of the Authority is published in a manner permitting remote access.

Section 138

(1) In fulfilment of tasks according to this Act the Authority shall be entitled

a) to process personal data to the extent necessary for fulfilment of tasks according to this Act;
b) to keep records of breach of protection of classified information, records of security directors (security officers), records of natural persons and facilities that have access to classified information, with the exception of members and employees placed in the Intelligence Services and selected policemen; records of natural persons who are holders of the Certificate, records of cryptographic protection staff, couriers of the cryptographic material and records of natural persons who are holders of the Specialist Competence Certificate;
c) to keep a certification file of the Information System, cryptographic equipment, cryptographic site and of the shielded chamber;
d) to require, free of charge, provision of information from the State body, legal person or the natural person pursuing business, and to use and record this information;
e) to require, for the purposes of the Procedure, from the Police and from the Intelligence Services information obtained by procedures according to the special legal regulation[43)];
f) to require a copy of criminal conviction records;
g) to inspect the criminal files;
h) to provide to the State body, legal person or natural person pursuing business to the extent necessary the requisite personal data relating to the information being requested;
i) to make a contract with the State body or facility to carry out partial tasks in certification of technical means, Information Systems, cryptographic equipment, cryptographic site, shielded chambers, to carry out training aimed at the Specific Specialist Competence of the cryptographic protection staff and to investigate the possibility of occurrence of compromising electromagnetic emissions where classified information will be stored or handled, and to produce cryptographic equipment;
j) to maintain data within its Information Systems obtained in the conduct of duties in accordance with this Act; and
k) to co-operate with the authority of the foreign power during the security clearance procedure having the jurisdiction in the area of protection of classified information, in particular to require information concerning the participant in the Procedure.

(2) Once a month the Authority shall provide to the Intelligence Services and to the Ministry of the Interior a list of issued PSCs, Certificates, and further a list of natural persons who have not been issued with the PSC or Certificate, as well as a list of persons in respect of whom the validity of the PSC or Certificate has been terminated.

Section 139

(1) The Authority shall process the proposal of the list of classified information. The government will issue the list of classified information by its decree.

(2) The list of classified information shall classify the respective classified information into one or more security classification levels according to S. 4.

Section 140
Intelligence Services

(1) The Intelligence Services shall

a) decide natural person applications in the case of their members, employees and job or service candidates, with the exception of job or service candidates who are holders of a personnel security clearance at least for the required security classification level, as well as the termination of validity of the security clearance of this natural person, and issue personnel security clearance according to S. 56 (a);

b) carry out acts upon the written request of the Authority within its jurisdiction during the course of the Procedure according to this Act.

(2) In deciding according to paragraph 1 the Intelligence Services shall have the position of the Authority and the responsible person of the Intelligence Service shall have the position of the director of the Authority. The responsibility for acts shall be in accordance with S. 5 of the Act N. 153/1994 Coll., to make provisions for the Intelligence Services of the Czech Republic, as amended.

(3) In performance of duties according to this Act the Intelligence Services shall report to the Authority without delay, whenever they discover circumstances indicating that the personal security clearance holder, FSC holder or Certificate holder no longer meets conditions for its issuance, provided that this notification will not endanger the interests pursued by the Intelligence Service.

(4) In conducting duties according to this Act the Intelligence Services shall be entitled

a) to use means for obtaining information according to the special legal regulations[44)];
b) to use data from their own records and data from records provided by the Authority;
c) to require and use data from records and materials developed in connection with activities of security and military bodies of the Czechoslovak state;
d) to process personal data;
e) to keep records;
f) to require, free of charge, information from the State body, legal person or natural person pursuing business and to use it;
g) to require a copy of criminal conviction records and statement of criminal records[11)];
h) to maintain data in the Information Systems obtained in the conduct of duties in accordance with this Act;
i) to implement measures relating to the register protection of personal data; and
j) to use data from the register of individuals who have been granted access to classified information according to S. 58 par. 4.

(5) The director of the Intelligence Service gives consent according to S. 59 par. 3.

Section 141
Ministry of the Interior and the Police

(1) The Ministry of the Interior shall decide a natural person application in the case of members of the Police selected in the interest of performance of important tasks of the Police by the Ministry of the Interior, with the exception of the Police members who are holders of a personnel security clearance at least for the required security classification level, as well as the termination of validity of the security clearance in the case of these Police members, and issue personnel security clearance according to S. 56 (a).

(2) In deciding according to paragraph 1 the Ministry of the Interior shall have the position of the Authority and the Minister of the Interior shall have the position of the director of the Authority.

(3) In performance of duties according to this Act the Ministry of the Interior shall further

a) report to the Authority without delay, whenever it discovers circumstances indicating that the PSC holder, FSC holder or Certificate holder no longer meets conditions for its issuance; and
b) implement, upon request of the Authority, measures relating to the register protection of personal data of the PSC holder or of his/her spouse, children and parents.

(4) In performance of duties according to paragraphs 1 to 3 the Ministry of the Interior shall be entitled

a) to use data from its registers as well as data provided by the Authority from its registers;
b) to process personal data;
c) to keep records
d) to require, free of charge, information from the State body, legal person or natural person pursuing business and to use it;
e) to require an opinion of the Police on the security eligibility of the selected member of the Police;
f) to require a copy of criminal conviction records and statement of criminal records[11)].

(5) The Police shall participate, within its competence according to the special legal regulation[30)], in performance of duties of the Ministry of the Interior according to paragraph 1; upon written request of the Authority it shall also carry out acts within its competence during the course of the Procedure.

(6) In performance of duties according to this Act, the Police shall be entitled to use data from the register of individuals granted access to classified information according to S. 58 par. 4.

(7) The Minister of the Interior gives consent according to S. 59 par. 3.

Section 142

(1) If any Document Found according to S. 65 par. 1 or Certificate found according to S. 87 par. 2 has been handed over to the Authority, to the Police or to the Embassy of the Czech Republic, the body concerned shall make the written record of its handing over, in which it shall identify the Document or Certificate Found, and it shall insert the name, surname, birth registration number (personal identity number) and the place of permanent residence of an individual who handed over the Document or Certificate Found, and, in detail, under what circumstances the individual concerned has obtained them. The Police or Embassy of the Czech Republic shall hand over the Document or Certificate Found to the Authority together with the record. The Authority shall forward classified information to its originator, and the PSC, FSC, Certificate, PSC for the foreign power, FSC for the foreign power shall be forwarded to the person or facility concerned, which have been issued with these documents.

(2) For the purposes of handing over of classified information according to paragraph 1, the member of the Police or the employee working on the Embassy of the Czech Republic shall be considered to be authorised to have access to classified information to the extent necessary for making the record and for the delivery of this classified information to the Authority.

PART SIX
STATE SUPERVISION

Section 143

(1) State supervision in the areas of protection of classified information and security eligibility means supervising how the State bodies, facilities and natural persons (hereinafter "the Controlled Persons") comply with legal regulations in this area.

(2) In the performance of the state control the procedure shall be in accordance with the Act regulating the state control[45)], as appropriate, save as otherwise provided herein.

(3) In the performance of the state supervision the employees of the Authority (hereinafter "the Supervising Staff") shall have access to classified information to the extent of the control being performed, if they display a valid PSC for the appropriate security classification level.

(4) The authority of the foreign power having jurisdiction over the protection of classified information shall be entitled to participate in the state supervision in the area of protection of classified information released by this authority to the Czech Republic, if it results from the obligation of the membership of the Czech Republic in the European Union, or if provided by the international agreement by which the Czech Republic is bound.

(5) In the cases according to S. 141 activities of the Intelligence Services and of the Ministry of the Interior shall not be subject to the state supervision as described herein.

Section 144

Remedial, corrective or disciplinary action

(1) Further to authorization according to the Act regulating the state control[45)], if the breach of legal regulations is ascertained in the areas of protection of classified information and security eligibility of the Controlled Person, the Supervising Staff are authorised to adopt necessary measures to ensure the protection of classified information, including withdrawal of classified information, measures to declassify or change the level of classified information or to mark classified information with the security classification level. The certificate of withdrawal shall be issued to the Controlled Person. The Supervising Staff are also authorised to require that remedial or corrective action shall be taken within a prescribed period to correct any deficiency being discovered.

(2) The Controlled Person shall meet costs of implementation of measures according to paragraph 1.

(3) In carrying out necessary measures according to paragraph 1 instruction of the Supervising Staff shall be complied with by each person.

(4) The Authority can impose a procedural fine for non-compliance with obligations according to paragraph 3 up to 100,000 CZK. The procedural fine can be imposed repeatedly. A collective sum of imposed procedural fines shall not exceed the amount of 400,000 CZK. S. 156 par. 3 and 7 to 9 will be applied for determination of the rate of the fine and of its maturity, and for collection and enforcing the payment of imposed fines.

PART SEVEN
CONTROL OVER ACTIVITIES OF THE AUTHORITY

Section 145

(1) Control over activities of the Authority shall be performed by the Chamber of Deputies that shall establish the special control body for this purpose (hereinafter "the Control Body").

(2) The Control Body shall be composed of seven members. Only a deputy of the Chamber of Deputies may be a member of the Control Body.

(3) The special legal regulation[46)] shall reasonably apply to discussions of the Control Body and to rights and obligations of its members, save as otherwise provided for in this Act.

(4) The members of the Control Body shall be permitted escorted access to the facilities of the Authority if accompanied by the director of the Authority or by an employee authorised by him/her.

(5) The director of the Authority shall submit to the Control Body

a) a report on activities of the Authority;
b) a report on individual Procedures with respect to the natural person application, facility application and Certificate application and on the termination of validity of a PSC, FSC or Certificate [S. 137 (a)];
c) a budget estimate of the Authority;
d) grounds necessary for the budgetary control of the Authority;
e) internal regulations of the Authority.

(6) The Control Body has no authorization to interfere with personal competences of chief officers of the Authority and to substitute their management activities.

Section 146

(1) If the Control Body considers that the activity of the Authority unlawfully restricts or infringes on the rights and liberties of citizens, or that decision-making activity of the Authority in the conduct of the security clearance procedure is affected by mistakes, it is entitled to ask for a necessary explanation from the director of the Authority.

(2) The notification shall be given to the director of the Authority and to the Prime Minister by the Control Body, of any breach of the law by an employee of the Authority in fulfilment of obligations according to this Act, discovered in carrying out its controlling activities.

Section 147

The obligation to hold information in confidence imposed on the members of the Control Body under this Act does not apply to cases when the Control Body submits notification according to S. 146 par. 2.

PART EIGHT
ADMINISTRATIVE DELICTS

Section 148

(1) The natural person commits an administrative infraction if

a) as the participant in the security clearance procedure, does not notify the change to the data contained in the natural person application according to S. 65 par. 3, or to the data contained in the Certificate application according to S. 87 par. 3;
b) does not hand over the Document Found according to S. 65 par. 1 or Certificate found according to S. 87 par. 2;
c) breaches the obligation to hold classified information in confidence;
d) allows access to classified information to an unauthorised person;
e) carries out functions of the security director (security officer) contrary to S. 71 par. 5 with more State bodies or facilities;
f) conducts cryptographic protection without being a member of the cryptographic protection staff fulfilling conditions set out in S. 38 par. 2;
g) operates the cryptographic equipment without meeting requirements set out in S. 40 par. 2;

h) transports cryptographic material without being the courier of the cryptographic material that meets requirements set out in S. 42 par. 1 or 2;
i) ensures that he/she may have access to classified information without meeting the conditions according to S. 6 par. 1 or S. 11 par. 1; or
j) leaves the territory of the Czech Republic with the certified cryptographic equipment without permission of the Authority.

(2) Fines can be imposed for administrative infractions up to

a) 50,000 CZK in the case of an administrative infraction according to paragraph 1 (a);
b) 100,000 CZK in the case of an administrative infraction according to paragraph 1 (b) or (e);
c) 500,000 CZK in the case of an administrative infraction according to paragraph 1 (f), (g) or (h);
d) 1,000,000 CZK in the case of an administrative infraction according to paragraph 1 (i);
e) 5,000,000 CZK in the case of an administrative infraction according to paragraph 1 (c), (d) or (j).

Section 149

(1) The natural person with access to classified information commits an administrative infraction if he/she

a) does not register or record classified information in administrative aids according to S. 21 par. 5;
b) makes a reproduction, copy or translation of classified information without consent as outlined in S. 21 par. 6;
c) hands over classified information contrary to S. 21 par. 8;
d) lends, transports or carries classified information contrary to S. 21 par. 7 or 9;
e) declassifies classified information or changes its security classification level without the consent of the originator or of the providing foreign power;
f) does not meet the conditions for processing or storing classified information according to S. 24 par. 5 or 6;
g) handles classified information in the Information System that has not been certified by the Authority or has not been certified for the respective security classification level or has not been approved in writing for the operation by the responsible person;
h) handles classified information in the Communication System, the security project of which has not been approved by the Authority or which has not been approved for the classification level of the communicated classified information;
i) processes classified information in the copying machine, display device or memory typewriter contrary to security operation guidelines issued according to S. 36 par. 2;
j) does not record cryptographic material in administrative aids of the cryptographic protection; or
k) handles cryptographic material contrary to S. 41 par. 2.

(2) Fines can be imposed for administrative infractions up to

a) 500,000 CZK in the case of an administrative infraction according to paragraph 1 (a), (b), (c), (d), (e), (f), (g) or (h);
b) 1,000,000 CZK in the case of an administrative infraction according to paragraph 1 (i), (j) or (k).

Section 150

(1) The natural person who is a holder of the PSC commits an administrative infraction if he/she

a) does not hand over the PSC, the validity of which was terminated, according to S. 66 par. 1 (b);
b) does not report the loss or theft of the PSC according to S. 66 par. 1 (c);
c) does not report immediately a change to the data entered in the attachment to the natural person application according to S. 94 par. 2 (a), (c) and (d);
d) does not hand over, as a holder of the PSC for the foreign power, PSC for the foreign power, the validity of which was terminated, according to S. 57 par. 8; or
e) does not report, as a holder of the PSC for the foreign power, loss or theft of his/her PSC for the foreign power according to S. 66 par. 1 (c).

(2) A fine of up to 50,000 CZK can be imposed for an administrative infraction according to paragraph 1.

Section 151

(1) The natural person who is a holder of the Notice commits an administrative infraction if he/she

a) does not report a change in conditions for the issuance of the Notice outlined in S. 6 par. 2 (a) and (c) or a change to the data contained in the Notice; or

b) does not hand over the Notice, the validity of which was terminated, according to S. 9 par. 6.

(2) The fine of up to 30,000 CZK can be imposed for an administrative infraction according to paragraph 1.

Section 152

(1) A natural person who is a holder of the Certificate commits an administrative infraction if he/she

a) does not hand over the Certificate, the validity of which was terminated, according to S. 87 par. 1 (a);
b) does not report the loss or theft of the Certificate according to S. 87 par. 1 (b); or
c) does not report the change to the data entered in the Certificate according to S. 87 par. 1 (c) or to the data in the Certificate application according to S. 87 par. 1 (d).

(2) A fine of up to 50,000 CZK can be imposed for an administrative infraction according to paragraph 1.

Section 153

(1) A legal person or natural person pursuing business with access to classified information or a State body commits an administrative infraction if he/she/it

a) does not provide the guards at the premises housing the security area classified as RESTRICTED, according to S. 28 par. 2 or 4;
b) does not prepare operation guidelines of the copying machine, display device or memory typewriter according to S. 36 par. 2;
c) does not secure the written authorization of the natural person to have access to classified information subject to Special Handling Regime, marked as "ATOMAL";
d) does not establish and staff a position of the security director (security officer) according to S. 71 par. 1;
e) does not report an appointment to the office of the security director (security officer) according to S. 71 par. 2;
f) does not mark elements on classified information according to S. 21 par. 2 to 4;
g) as the originator, marks the security classification level on the information that is not included on the list of classified information, or on information whose divulgence or misuse cannot cause damage to the interests of the Czech Republic or cannot be unfavourable to these interests;
h) as the originator, does not notify declassification of or change to the classification according to S. 22 par. 6;
i) as the addressee of classified information, does not notify declassification of or change to the classification according to S. 22 par. 6;
j) does not provide continuing guards at the premises according to S. 28 par. 1, 3 or 4 housing the security area or area designated as the meeting room;
k) does not report the breach of obligations in the protection of classified information;
l) does not prepare the physical security project according to S. 32;
m) does not maintain some of records as outlined in S. 69 par. 1 (j);
n) does not hand over classified information to be recorded according to S. 69 par. 1 (n);
o) does not ensure that implemented measures of the physical security correspond with the physical security project and the requirements set out according to S. 31;
p) as the originator, does not mark the elements according to S. 21 par. 1 and 4, although the information is included on the list of classified information and its divulgence or misuse can cause damage to the interests of the Czech Republic or can be unfavourable to these interests;
q) as the originator, does not immediately declassify or change the classification level in the cases when reasons will extinguish for classification of the information, the reasons for classification do not correspond to the assigned security classification level or if the security classification level has been assigned without authorization;
r) does not ensure that conditions have been created as outlined in S. 33 for storing and in S. 23 par. 2 for accounting, lending or transportation of classified information or classified information requiring a Special Handling Regime, or for other forms of handling;
s) operates the Information System that has not been certified by the Authority or approved in writing for operation by a responsible person;
t) operates the Communication System whose security project has not been approved by the Authority;
u) does not terminate the operation of the Information System that does not meet the conditions laid down in the certification report or does not terminate the operation of the Communication System that does not meet

conditions laid down in the Communication System security project;

v) uses an equipment for the cryptographic protection that has not been certified by the Authority, or uses the cryptographic site for purposes other than for those it has been certified and approved for operation;
w) does not ensure that the cryptographic protection will be performed by an individual who complies with requirements laid down in S. 38 par. 2;
x) does not ensure that the cryptographic equipment will be operated by an individual who complies with requirements laid down in S. 40 par. 2;
y) does not ensure that the cryptographic material will be transported by an individual who complies with requirements laid down in S. 42 par. 1 or 2;
z) does not report the compromise of cryptographic material according to S. 43 par. 2;
aa) does not establish the Registry or does not report changes in the Registry to the Authority according to S. 79 par. 7 (d);
bb) does not carry out the inventory of classified information maintained in the Registry according to S. 69 par. 1 (m) or does not notify the Authority of its result;
cc) sends classified information at the security classification level TOP SECRET, SECRET or CONFIDENTIAL contrary to S. 77; or
dd) allows performance of activities of a sensitive nature to the natural person who is not a holder of the valid Certificate.

(2) The following fine will be imposed for administrative infractions up to

a) 300,000 CZK in the case of an administrative infraction according to paragraph 1 (a), (b), (c), (d), (e), (f) or (g);
b) 500,000 CZK in the case of an administrative infraction according to paragraph 1 (h), (i), (j), (k), (l), (m), (n) or (o);
c) 1,000,000 CZK in the case of an administrative infraction according to paragraph 1 (p), (q), (r), (s), (t), (u), (v), (w), (x), (y), (z), (aa), (bb), (cc) or (dd).

Section 154

(1) The facility with access to classified information commits an administrative infraction if it

a) does not hand over or forward classified information according to S. 56 par. 2;
b) does not update the facility security documents according to S. 98;
c) provides classified information at the level RESTRICTED to a foreign partner contrary to S. 73 (b);
d) provides classified information at the level TOP SECRET, SECRET or CONFIDENTIAL to a foreign partner contrary to S. 73 (a); or
e) leaves the territory of the Czech Republic with a certified cryptographic equipment without the permission of the Authority.

(2) A fine will be imposed for administrative infractions up to

a) 1,000,000 CZK in the case of an administrative infraction according to paragraph 1 (a), (b) or (c);
b) 5,000,000 CZK in the case of an administrative infraction according to paragraph 1(d) or (e).

Section 155

(1) The facility that is a holder of the FSC commits an administrative infraction if it

a) does not forward, according to S. 68 (a), the FSC, validity of which was terminated;
b) does not report, according to S. 68 (b), the loss or theft of the FSC;
c) does not report, according to S. 68 (c), any change to the data as stipulated by S. 97 (a) and (b);
d) does not report, according to S. 68 (d), any change to the data in the attachment to the facility application according to S. 96 par. 2 (a) and (b);
e) as a holder of the FSC for a foreign power, does not hand over, according to S. 57 par. 8, a FSC for a foreign power, the validity of which was terminated;
f) as a holder of the FSC for a foreign power, does not report, according to S. 68 (b), the loss or theft of a FSC for a foreign power; or
g) does not secure the protection of classified information, upon termination of validity of the FSC as outlined in S. 56 par. 2.

(2) A fine will be imposed for administrative infractions up to

a) 50,000 CZK in the case of administrative infraction according to paragraph 1 (a), (b), (c), (d), (e) or (f);
b) 100,000 CZK in the case of administrative infraction according to paragraph 1 (g).

Section 156
Common provisions

(1) A legal person will not be liable for an administrative delict if it satisfies that it has made every reasonable effort to prevent the breach of legal obligations.

(2) The liability of the legal person for an administrative infraction shall extinguish if the Authority did not initiate proceedings against the administrative infraction within one year from the date on which it became aware of this, but within three years at the latest from the date when the administrative infraction has been committed.

(3) The seriousness of an administration infraction shall be taken into account in determining the rate of the fine, in particular the mode of its committing and its consequences, as well as circumstances of its committing.

(4) Provisions of this Act, regulating the liability of the legal person, shall be applied for assessment of liability for practices in the area of protection of classified information at the time of pursuing business of a natural person[9)] or in direct relation to this business, as well as for an administrative proceedings to deal with the breach of obligations of the natural person pursuing business in the area of protection of classified information.

(5) In the case of administrative proceedings to deal with the breach of obligation of the natural person in the area of protection of classified information that did not occur during his/her business activities or in direct relation to this business, the provisions of the act to make provisions for the administrative infractions[47)] shall be applied.

(6) The Authority shall hear administrative delicts according to this Act.

(7) Fines shall be collected by the Authority and enforced by the customs authority. The proceeds from fines shall be used for the state budget revenue.

(8) Fines shall be due within 30 days from the date a decision to impose the fine comes into force.

(9) Enforcing the payment of imposed fines shall be in accordance with the act regulating the administration of taxes[48)].

PART NINE
TRANSITIONAL AND FINAL PROVISIONS

Section 157
Transitional provisions

(1) Classified information according to current legal regulations shall be considered to be classified information according to this Act. If classified information or state and official secrets are mentioned in the existing legal regulations these shall mean classified information according to this Act.

(2) The security classification level established according to existing legal regulations shall be considered to be security classification level established according to this Act.

(3) The security classification levels of classified documents originated before 31 December 1992 shall be cancelled as from the 1 January 2008, unless otherwise specified in particular cases by the responsible person until 31 December 2007.

(4) Written records of designation according to existing legal regulations shall be considered to be the briefing according to this Act.

(5) A security clearance certifying that the person concerned meets conditions prescribed for its issuance, which has been granted according to existing legal regulations, shall be considered to be the PSC according to this Act until expiration of its validity indicated therein.

(6) A certificate of the security eligibility of the natural person that has been issued according to existing legal regulations shall be considered to be the certificate of the security eligibility of a natural person according to this Act, including the period of its validity.

(7) The notice of fulfilment of conditions for the purposes of designation of the individual concerned for the classification level RESTRICTED that has been issued according to existing legal regulations shall be considered to be verification of fulfilment of conditions of legal capacity, age and integrity for the period of six months from the effective date of this Act, required for giving access to a natural person to classified information at the classification level RESTRICTED according to this Act, provided that the responsible person or classified information provider takes steps to brief the natural person

concerned within one month from the effective date of this Act.

(8) Approval to the designation of the person concerned without prior security clearance procedure, which has been given according to existing legal regulations, shall be considered to be the approval to access to classified information on a one-time basis for a period of six months from the effective date of this Act for the classification level to which he/she is to be issued with the security clearance.

(9) The natural person who had been authorised to have access to classified information according to existing legal regulations before the effective date of this Act only on the basis of the briefing and who had not been a holder of the valid security clearance, may be authorised to have access to classified information from the effective date of this Act only if he/she is a holder of a valid PSC. This requirement does not apply in the case of persons who are authorised to have access to classified information according to this Act without a valid PSC and without a briefing.

(10) The certificate confirming to a foreign power that the person concerned has been issued with a security clearance or that the organization has been issued with a confirmation, which was issued according to existing legal regulations, shall be considered to be the PSC for the foreign power or the FSC for the foreign power until expiration of its validity indicated therein, confirming to the foreign power that the security clearance procedure had been conducted in the case of a natural person or facility and that the natural person is a holder of a PSC or the facility is a holder of a FSC for the given classification level, and in the case of the FSC also the forms in which classified information can be found.

(11) The confirmation that the facility meets conditions prescribed for its issuance, which has been issued according to existing legal regulations, shall be considered to be the FSC according to this Act until expiration of its validity indicated therein.

(12) The consent to exchange classified information between the organization and the foreign partner that has been given according to existing legal regulation shall be considered to be the permission to exchange classified information between the organization and the foreign partner outside the territory of the Czech Republic according to this Act.

(13) The specialist competence certificate of a cryptographic protection officer that has been issued according to existing legal regulations shall be considered to be the specialist competence certificate of a cryptographic protection officer according to this Act until expiration of its validity indicated therein.

(14) The certificate of technical means used for the protection of classified information that has been issued according to existing legal regulations shall be considered to be the technical means certificate according to this Act until expiration of its validity indicated therein.

(15) The certificate of the Information System used for handling classified information that has been issued according to existing legal regulations shall be considered to be the Information System certificate according to this Act until expiration of its validity indicated therein.

(16) The certificate of the cryptographic equipment used for protection of classified information that has been issued according to existing legal regulations shall be considered to be the cryptographic equipment certificate according to this Act until expiration of its validity indicated therein.

(17) The classified security standard that has been issued according to existing legal regulations shall be considered to be the security standard according to this Act.

(18) The security clearance procedure initiated before the effective date of this Act will be completed in accordance with existing legal regulations. The time to perform the comparable security clearance procedure according to this Act shall apply to its completion, with the understanding that the time begins to run from the effective date of this Act.

(19) The verification of the security eligibility initiated before the effective date of this Act will be completed according to existing legal regulations. The time to perform the verification according to this Act shall apply to its completion, with the understanding that the time begins to run from the effective date of this Act.

(20) The process of technical means certification, Information System certification or the cryptographic equipment certification initiated before the effective date of this Act will be completed in accordance with this Act.

(21) A complaint lodged against the non-issuance of the security clearance, confirmation or the

Certificate before the effective date of this Act shall be disposed of according to existing legal regulations.

(22) An application for remedial measure brought according to existing legal regulations to the Collegium in the area of protection of classified information, which has not been decided before the effective date of this Act, will not be disposed of by the Collegium any more. In this case the Collegium will return all files to the body that brought it within five days from the effective date of this Act. This body shall instruct the participant in the Procedure in writing of the possibility to bring an action against the decision of the director of the Authority; in these cases the time-limit for bringing the action shall run again from the date of the service of the written instruction.

(23) An action may be brought according to this Act against the decision to dismiss the complaint issued according to existing legal regulations after the effective date of this Act.

(24) The proceedings to impose a fine initiated before the effective date of this Act will be completed according to existing legal regulations.

(25) The Communication System that has been operated before the effective date of this Act may be operated until such time as its security project has been approved, but for no longer than 12 months from the effective date of this Act, provided that the responsible person of the body requests, in writing, approval of its security project within three months from the effective date of this Act.

(26) The site, on which the activities associated with the cryptographic protection were performed before the effective date of this Act, may be used for performance of cryptographic protection until such time that it has been approved for operation by the authorised representative, but for no longer than 12 months from the effective date of this Act; and if the site is subject to certification, provided that the State body or facility request in writing certification within three months from the effective date of this Act.

(27) The shielded chamber that has been used by the Ministry of Foreign Affairs at the Embassy of the Czech Republic for the protection of classified information before the effective date of this Act may be used by this Ministry for the protection of classified information until such time that it has been certified, but for no longer than 24 months from the effective date of this Act, provided that the Ministry of Foreign Affairs requests in writing its certification within three months from the effective date of this Act.

(28) Carrying out security investigation on a natural person, or an organization, technical means certification, Information System certification, cryptographic equipment certification, verification of the security eligibility of the natural person, issuance of the certificate confirming to a foreign power that the person concerned has been issued with a security clearance or the organization with the confirmation, and issuance of consent to exchange classified information between the organization and a foreign partner shall be governed by existing legal regulations only if the application has been consigned to the post or otherwise delivered or consigned no later than 45 days prior to the effective date of this Act.

Section 158
Delegating provisions

The Authority shall issue the regulation to implement S. 7 par.3, S. 9 par. 8, S. 23 par. 2, S. 33, S. 34 par. 5, S. 35 par. 5, S. 36 par. 5, Ss. 44, 53 and 64, S. 79 par. 7, S. 85 par. 5 and S. 135.

Section 159
Relation to the Rules of Administrative Procedure

Rules of Administrative Procedure relates only to the procedure according to Part two Chapter IX, save as otherwise provided in this Chapter, and according to Part eight.

Section 160
Repealing clause

The following shall be hereby repealed:

1. Act. N. 164/1999 Coll., to alter Act N. 148/1998 Coll., on Protection of Classified Information and on Amendments to Relevant Legislation.
2. Act N. 363/2000 Coll., to alter Act N. 148/1998 Coll., on Protection of Classified Information and on Amendments to Relevant Legislation, as amended.
3. Act N. 386/2004 Coll., to alter Act N. 148/1998 Coll., on Protection of Classified Information and on Amendments to Relevant Legislation, as amended.
4. Decree of the Government N. 340/2002 Coll., to lay down the list of some sensitive activities.
5. Decree of the Government N. 385/2003 Coll., to lay down the sensitive activity for the Castle Guard.

6. Decree of the Government N. 31/2005 Coll., to lay down the list of some sensitive activities for civil aviation, as amended by the Decree of the Government N. 212/2005 Coll.
7. Decree of the Government N. 246/1998 Coll., to lay down the lists of classified information.
8. Decree of the Government N. 89/1999 Coll., to alter the Decree of the Government N. 246/1995 Coll., to lay down the lists of classified information.
9. Decree of the Government N. 152/1999 Coll. to alter the Decree of the Government N. 246/1998 Coll., to lay down the lists of classified information, as amended by the Decree of the Government N. 89/1999 Coll.
10. Decree of the Government N. 17/2001 Coll., to alter the Decree of the Government N. 246/1998 Coll., to lay down the lists of classified information, as amended.
11. Decree of the Government N. 275/2001 Coll., to alter the Decree of the Government N. 246/1998 Coll., to lay down the lists of classified information, as amended.
12. Decree of the Government N. 403/2001 Coll., to alter the Decree of the Government N. 246/1998 Coll., to lay down the lists of classified information, as amended.
13. Decree of the Government N. 549/2002 Coll., to alter the Decree of the Government N. 246/1998 Coll., to lay down the lists of classified information, as amended.
14. Decree of the Government N. 631/2004 Coll., to alter the Decree of the Government N. 246/1998 Coll., to lay down the lists of classified information, as amended.
15. Regulation N. 137/2003 Coll., regulating details of establishing and marking of the security classification level and of providing the administrative security.
16. Regulation N. 245/1998 Coll., to make provisions for personal eligibility and formats of forms used in the area of personal security.
17. Regulation N. 397/2000 Coll., to alter the Regulation N. 245/1998 Coll., to make provisions for personal eligibility and formats of forms used in the area of personal security.
18. Regulation N. 263/1998 Coll., to lay down the method and verification procedure of the security eligibility of the organization.
19. Regulation N. 12/1999 Coll., to provide for the technical security of classified information and to make provisions for the certification of technical means.
20. Regulation N. 337/1999 Coll., to alter the Regulation N. 12/1999 Coll., to provide for the technical security of classified information and to make provisions for the certification of technical means.
21. Regulation N. 56/1999 Coll., to provide for the security of Information Systems handling classified information, to make provisions for carrying out their certification and for elements of the certificate.
22. Regulation N. 339/1999 Coll., to make provisions for physical security.
23. Regulation N. 136/2001 Coll., to provide for the cryptographic protection of classified information, to make provisions for carrying out cryptographic equipment certification and for elements of the certificate.
24. Regulation N. 348/2002 Coll., to make provisions for security eligibility of natural persons.

Section 161
Coming into force

This Act comes into force on 1 January 2006.

Signed

Vlček

Klaus

Topolánek

CONTENTS

[1)] E.g. S.3 of the Act. N. 219/2000 Coll., to make provisions for the property of the Czech Republic and its acting in legal relations, S.2 par. 7 of the Act N. 238/2000 Coll., to make provisions for the Fire-brigade of the Czech Republic and altering some other laws, S. 55b par. 3 of the Act N. 49/1997 Coll., to make provisions for the civil aviation and to alter and amend Act N. 455/1991 Coll., Act to regulate trades (Trade Act), as amended, as amended by the Act N. 258/2002 Coll.
[2)] Act N. 129/2000 Coll., Regions Act (Position of Regions), as amended.
[3)] Act N. 131/2000 Coll., Capital City of Prague Act, as amended.

[4)] Act N. 128/2000 Coll., Communities Act (Position of Communities), as amended.
[5)] Act N. 154/1994 Coll., Security Intelligence Service Act, as amended.
[6)] Act N. 289/2005 Coll., Military Intelligence Act, as amended.
[7)] Act N. 6/1993 Coll., Czech National Bank Act, as amended.
[8)] The Commercial Code.
[9)] S. 2 par. 2 of the Commercial Code.
[11)] Act. N. 269/1994 Coll., Criminal Records Act, as amended by Act N. 126/2003 Coll.
[12)] S. 68 par. 1 of the Act N. 499/2004 Coll., regulating records archive and documents service, and altering some other laws.
[13)] S. 3 of the Act N. 153/1994 Coll., Intelligence Services of the Czech Republic Act.
[14)] S. 68 of the Commercial Code.
[15)] Act N. 182/2006 Coll., Act on Insolvency and its Resolution (Insolvency Act), as amended.
[16)] Cancelled.
[17)] Act N. 29/2000 Coll., to make provisions for postal services and to alter some other acts (the Postal Services Act), as amended.
[18)] S. 7 and consequential sections of the Act N. 499/2004 Coll.
[19)] S. 10 of the Act N. 153/1994 Coll.
[20)] Act. N. 240/2000 Coll., to make provisions for crisis situation management and to alter some other laws (Crisis Act), as amended.
[21)] E.g. S. 14 par. 3 of the Act N. 219/1999 Coll., Armed Forces of the Czech Republic Act, S. 50(a)a par. 1 of the Act N. 283/1991, Police of the Czech Republic Act, as amended by the Act N. 26/1993 Coll.
[22)] Act N. 227/2000 Coll., to make provisions for electronic signature and to alter some other laws (Electronic Signature Act), as amended.
[24)] S. 18 par. 1 of the Act N. 153/1994 Coll.; S. 15 par. 2 of the Act N. 154/1994 Coll.
[25)] S. 33 (f) of the Act N. 13/1993 Coll., Customs Act, as amended by the Act N. 1/2002 Coll.; S. 23 (f) of the Act N. 283/1991 Coll., as amended by Act N. 265/2001 Coll.
[26)] Act N. 137/2001 Coll., Act to provide the special protection of witness and another persons in connection with criminal proceedings, and to alter the Act N. 99/1963 Coll., Civil Procedure Act, as amended.
[27)] Act N. 361/2003 Coll., regulating service relationship of members of security forces, as amended.
[28)] Criminal Procedure Code; Civil Procedure Code; Rules of the Administrative Procedure.
[28a)] S. 69 of the Commercial Code.
[29)] For example the Act N. 218/2002 Coll., regulating the service of state employees in administrative offices and regulating remuneration of these employees and other employees in administrative offices (Civil Service Act), as amended, Act. N. 312/2002 Coll., to make provisions for officers of territorial self-governing units and to alter some other laws, as amended by Act N. 46/2004 Coll., regulation N. 50/1978 Coll., to make provisions for specialist competence in electrotechnics, as amended by regulation N. 98/1982 Coll.
[30)] For example Act N. 283/1991 Coll, as amended, Act N. 137/2001 Coll.
[31)] For example S. 47a par. 6 of the Act N. 283/1991 Coll., as amended, S. 21 par. 1 of the Act N. 137/2001 Coll.
[32)] For example Act. N. 38/1994 Coll., to make provisions for foreign trades in military materials and to make provisions for supplementing of the Act N. 455/1991 Coll., to regulate trades (Trade Act), as amended, and of the Act N. 140/1961 Coll., Penal Code, as amended, as amended, Act N. 18/1997 Coll., to make provisions for peace use of nuclear energy and ionising radiation (atomic law) and for altering and supplementing some other laws, as amended.
[33)] Act N. 273/2001 Coll., to provide rights of members of national minorities and to alter some other laws, as amended by the Act N. 320/2002 Coll.
[34)] Act N. 41/1993 Coll., to regulate authentication of identity of duplicates or copies with the document, and to regulate verifying the authenticity of the signature by District Offices and community bodies and to regulate issuance of confirmation by community bodies and District Offices, as amended.
[35)] Act N. 167/1998 Coll, to make provisions for habit-forming substances and to alter and amend some other laws, as amended.
[36)] S. 115 of the Commercial Code.
[37)] S. 18 of the Act N. 563/1991 Coll., to make provisions for book keeping, as amended.
[38)] S. 3 of the Act N. 586/1992 Coll., to make provisions for income tax return, as amended.
[39)] S. 116 of the Civil Code.
[40)] Act N. 119/1992 Coll., to regulate travelling expenses, as amended.

[41] Act N. 36/1967 Coll., Experts and Interpreters Act.
[42] Judicial Rules of Administrative Procedure.
[43] Act N. 153/1994 Coll., as amended; Act N. 283/1991 Coll., as amended.
[44] Act N. 153/1994 Coll., as amended.
[45] Act N. 552/1991 Coll., regulating state control, as amended.
[46] Act N. 90/1995 Coll., regulating standing rules of a Chamber of Deputies, as amended.
[47] Act N. 200/2000 Coll., to make provisions for the administrative infractions, as amended.
[48] Act N. 337/1992 Coll., regulating administration of taxes and charges, as amended.