

Regulation N. 523 of 5 December 2005

on the Security of Information and Communication Systems and other Electronic Devices Handling Classified Information, and on the Certification of Shielded Chambers

Legal Disclaimer

The following text is a translation of the original promulgated in the Czech language in the Collection of Laws. This translated version has been effected by the National Security Authority of the Czech Republic and it cannot be relied on as an authentic wording, nor does it cause any legal effects. Any liability of the author is hereby excluded.

The National Security Authority lays down the following according to S. 34 par. 5, S. 35 par. 5, S. 36 par. 5 and S. 53(a), (b), (c), (d), (g), (h), (i) and (j) of the Act N. 412/2005 Coll., on the Protection of Classified Information (hereinafter “the Act“):

PART ONE INTRODUCTORY PROVISIONS

Section 1 Subject of legislation

This Regulation shall determine requirements for information systems handling classified information¹ (hereinafter “the Information System” and the process of their certification, requirements for communication systems handling classified information (hereinafter “the Communication System”) and the process of approval of their security projects, the protection of classified information in a copying machine, display device and memory typewriter, the protection of classified information from its leakage through compromising electromagnetic emissions and the process of certification of shielded chambers.

Section 2 Definition of terms

The following definitions shall apply for the purposes of this Regulation

- a) assets of the Information System on the basis of risks analysis (S 11) – a defined hardware, software, Information System documentation and

¹ S. 34 of the Act N. 412/2005 Coll., on the Protection of Classified Information.

- classified information stored in the Information System;
- b) object of the Information System – a passive element of the Information System that contains or receives information;
- c) subject of the Information System – active element of the Information System that causes transmission of information between objects of the Information System or a change in the state of the system;
- d) risks analysis – a process in which assets of the Information System are sought, threats influencing the assets of the Information System, its vulnerabilities, probability of the threats actuation and assessment of consequences arising from these threats;
- e) audit trail – record of the Information System of an event that may affect security of the Information System;
- f) identification of the Information System subject – a process of determining of its identity in the Information System;
- g) authentication of the Information System subject – a process of verification of its identity in the Information System, which satisfies required assurance level;
- h) authorization of the Information System subject – granting of certain rights to perform specified activities in the Information System;
- i) confidentiality of classified information – a property that classified information cannot be disclosed to any unauthorised person;
- j) physical security of the Information System or the Communication System – measures to ensure the physical protection of these systems against threats, whether accidental or intentional;
- k) integrity of the Information System or the Communication System asset – a property that

- enables its change in a specified manner and the change may be made only by authorised subject of the Information System;
- l) communication security - measures used to ensure the protection of classified information during its transmission through defined communication environment;
 - m) computer security – security of the Information System provided by its technical and program means;
 - n) mandatory access control – means restricting access of subjects of the Information System to objects of the Information System based on the comparison of classification of classified information contained in the object of the Information System and the level of authorisation of the subject of the Information System to have access to classified information, and ensuring the correct information flow between the objects of the Information System of mixed classification independently of a preference expressed by a user;
 - o) risk to the Information System or the Communication System - the likelihood of Communication and Information System's vulnerabilities being exploited by the threats;
 - p) role – a summary of determined activities and necessary authorizations for the subject of the Information System operating in the Information System or in the Communication System;
 - q) security officer of the Information System or the Communication System – an officer of the Information System or the Communication System administration in the role created for the management and control of the Information System or the Communication System security and conducting determined activities aimed at securing the safety of the Information System or the Communication System;
 - r) Information System administrator or Communication System administrator – an officer of the Information System or the Communication System administration in the role created specifically for ensuring the required functionality of the Information System or the Communication System and operation management of the Information System or the Communication System;
 - s) user of the Information System or user of the Communication System – a natural person fulfilling the role created specifically for handling classified information in the Information System or for transmission of classified information in the Communication System;
- t) access control - means restricting access of subjects of the Information System to objects of the Information System, ensuring that only authorised subject of the Information System may obtain access to these objects;
 - u) optional access control - means restricting access of subjects of the Information System to objects of the Information System based on the check of access rights of the subject of the Information System to the object of the Information System, and a user, administrator or security officer of the Information System having certain access rights to the object of the Information System may select which other subjects of the Information System will be authorised by him/her to have access to this object of the Information System, being such in a position to affect the information flow between the objects of the Information System;
 - v) security standard – classified set of rules determining procedures, technical solutions, security parameters and organizational measures in order to provide the minimum possible level of protection of classified information;
 - w) security mode of operation – the environment, in which the Information System operates and which is characterized by the classification level of classified information being processed and levels of users' authorizations;
 - x) applicant – a State body or a facility that submitted an application to the National Security Authority (hereinafter “the Authority”) to certify the Information System, the shielded chamber, to approve the Communication System security project or to verify capability of electrical and electronic devices, the security area or facility to ensure protection from any leakage of classified information through compromising electromagnetic emissions.

PART TWO INFORMATION SYSTEM

CHAPTER I INFORMATION SYSTEMS SECURITY REQUIREMENTS

Section 3 Information Systems security

(1)The Information System security will be achieved by application of the set of measures from the following areas

- a) computer and communication security;
- b) cryptographic protection;
- c) protection from leakage of compromising electromagnetic emissions;
- d) administration security and organizational measures;
- e) personnel security; and
- f) physical security of the Information System.

(2)Measures implemented during the process of certification of the Information System shall ensure that risks from specific threats and vulnerabilities against the Information System will be mitigated to the extent possible.

(3)The set of measures laid down in paragraph 1 shall be specified in the security documentation of the Information System.

Section 4

Security documentation of the Information System

(1)The security documentation of the Information System shall be composed of

- a) project security documentation of the Information System; and
- b) operational security documentation of the Information System.

(2)The project security documentation of the Information System shall contain the following

- a) Information System security policy and results of the risks analysis;
- b) proposal of the security of the Information System ensuring that the Information System security policy will be met, where details of its description shall make a direct implementation of measures being proposed possible; and
- c) documentation concerning tests of the Information System security.

(3)The operational security documentation of the Information System shall contain the following

- a) security instructions of the Information System specifying activities of Information System

security officers in roles established in the Information System aimed at providing the security administration of the Information System;

- b) security instructions of the Information System specifying activities of Information System administrators in roles established in the Information System for the Information System administration, if these activities are aimed at providing security of the Information System; and
- c) security instructions of the Information System specifying activities of Information System users, if these activities are aimed at providing security of the Information System.

Section 5

Information System security policy

(1)A security policy shall initially be produced during development of each Information System. The Information System security policy shall be composed of a set of standards, rules and procedures, which shall define a manner in which confidentiality, integrity and availability of classified information is to be provided, as well as responsibility of a user, security officer and Information System administrator for their functioning in the Information System. Principles of the security policy shall be detailed in the project and operational documentation of the Information System.

(2)International standardised security specifications² may also be used in formulation of the Information System security policy and evaluating of security properties of components of the Information System.

Section 6

Requirements for formulation of the Information System security policy

The Information System security policy shall be formulated on the basis of

- a) minimum security requirements in the area of computer security;
- b) system-dependent security requirements, requirements of a user and results of risks analysis; and

² E.g. ČSN ISI/IEC 15408 ITSEC - Information Technology Security Evaluation Criteria.

- c) security requirements of the security policy of a superior body, if available.

Section 7

Minimum security requirements in the area of computer security

(1) The Information System handling classified information classified CONFIDENTIAL or above shall ensure the following security functions

- a) unambiguous identification and authentication of the user, security officer or the Information System administrator, which shall precede all their other activities in the Information System and ensure the protection of confidentiality and integrity of authentication information;
- b) optional control of access to objects of the Information System on the basis of differentiation and administration of access rights of an user, security officer or the Information System administrator, and on the basis of their identity or membership in a group of users, security officers or the Information System administrators;
- c) continuous recording of events, which could affect security of the Information System, into audit records and safeguarding of audit records from an unauthorised access, in particular from its modification or destruction. In particular any use of identification and authentication information, attempted searching of access rights, establishment or disestablishment of the object of the Information System or activities of authorised subjects of the Information Systems affecting the security of the Information System shall be recorded;
- d) possibility of searching of audit records and designation of responsibility of an individual user, security officer or the Information System administrator;
- e) securing of memory objects prior to their further use, in particular prior to distribution to other subject of the Information System so as to ensure that they cannot be reconstructed and made readable again; and
- f) protection of confidentiality of data during transmission between the source and the target.

(2) Identifiable software hardware mechanisms shall be implemented in the Information System to provide security functions outlined in paragraph 1. Documentation describing their design and

operational setting shall enable their independent verification and evaluation of their sufficiency.

(3) Security mechanisms to implement security functions ensuring that the Information System security policy will be applied, shall be protected from any breach or unauthorised changes throughout all the lifecycle.

(4) Security functions outlined in paragraph 1 shall be appropriately used in the Information System handling classified information classified up to RESTRICTED level, and measures from the area of personnel, administrative and physical security of Information Systems.

Section 8

System-dependent security requirements based on the security operational mode

(1) Information Systems may be operated only in some of the following security modes of operation

- a) Dedicated security mode of operation;
- b) security mode of operation System High; or
- c) security mode of operation Multi-Level.

(2) The Dedicated security mode of operation is such an environment that permits processing of classified information of mixed classification and in which all users must fulfil conditions for access to the highest classification level of information stored within the Information System and all users must have common need-to-know for all classified information stored within the Information System. Minimum security requirements in the area of computer security requirements outlined in S. 7 par. 1 (a), (c), (d) and (f) shall be fulfilled, and measures from the area of administrative and personnel security and physical security of Information Systems shall be implemented to safeguard security of the Information System, which is operated in the Dedicated security mode of operation. The level of measures used from the mentioned areas and of measures to ensure confidentiality of data during its transmission must be at least equal to the level required for the highest classification of classified information being handled in the Information System.

(3)The security mode of operation System High is such an environment that permits simultaneous processing of classified information of mixed classification, in which all users must fulfil conditions for access to the highest classification level of information stored within the Information System, and not all users need a common need-to-know for all classified information. Minimum security requirements in the area of computer security requirements outlined in S. 7 shall be fulfilled and measures from the area of administrative and personnel security and physical security of Information Systems shall be implemented to safeguard security of the Information System, which is operated in the security mode of operation System High. The level of measures used from the mentioned areas and of measures to ensure confidentiality of data during its transmission must be at least equal to the level required for the highest classification of classified information being handled in the Information System.

(4)The security mode of operation Multi-Level is such an environment that permits simultaneous processing of classified information of mixed classification within one Information System, in which not all users must fulfil conditions for access to the highest classification level of information stored within the Information System, and not all users need a common need-to-know for all classified information. Measures outlined in paragraph 3 shall be implemented and a security function of mandatory access control of subjects of the Information System to objects of the Information System shall be established to safeguard security of the Information System, which is operated in the security mode of operation Multi-level. The level of measures to be used from the area of administrative and personnel security, physical security of Information Systems and of measures to ensure confidentiality of data during its transmission must be determined on the mandatory access control principle.

(5)A function of mandatory control of access to objects of the Information System by subjects of the Information System shall ensure

- a) constant connection of each subject of the Information System and object of the Information System with security attribute, which for the subject of the Information System indicates the level of authorization of the subject of the

- Information System and for the object of the Information System its classification level;
- b) integrity protection of the security attribute;
 - c) exclusive authorization of a security officer of the Information System to carry out changes in security attributes of subjects of the Information System, as well as of objects of the Information System;
 - d) assignment of pre-defined values of attributes for newly created objects of the Information System and keeping of attribute when copying object of the Information System.

(6)The following principles shall be secured when the security function of mandatory control of access to objects of the Information System by subjects of the Information System is applied

- a) a subject of the Information System may read information in an object of the Information System only if the level of his/her/its authorization is commensurate with the classification of the object of the Information System or above;
- b) a subject of the Information System may record information to an object of the Information System only if the level of his/her/its authorization is commensurate with the classification of the object of the Information System or below; and
- c) access to information contained in an object of the Information System by a subject of the Information System will be possible if permitted both by rules of mandatory access control and by rules of optional access control.

(7)The Information System that is operated in the security mode of operation Multi-Level, shall be capable to classify correctly output classified information from the Information System and enable to classify input classified information to the Information System.

(8)The Information System that is operated in the security mode of operation Multi-Level and that handles TOP SECRET classified information shall be identified and analysis shall be made of covert channels. The term covert channel includes non-permissible communication which could cause disclosure of classified information to an unauthorized subject of the Information System.

Section 9

System-dependent security requirements in computer networks environment

(1)The protection of confidentiality and integrity of classified information shall be ensured during its communication channel transmission.

(2)The cryptographic protection³ shall be the basic means to secure confidentiality of classified information during its communication channel transmission.

(3)The positive detection of deliberate and inadvertent modifications of classified information shall be the basic means to ensure integrity of classified information during its communication channel transmission.

(4)The physical protection of all components of a communication channel can be sufficient for a local area network within the frame of the security area or facility.

(5)The positive identification and authentication of communicating parties shall be secured, depending on a communication environment, including the protection of identification and authentication information. This identification and authentication shall precede the transmission of classified information.

(6)Connection of a network, which is under control of the Information System administration to the public network, which is not under control of the Information System administration, shall be secured by suitable security interface in such a manner as to prevent any cross-talks.

Section 10

Requirements for availability of classified information and services of the Information System

(1)The Information System shall ensure that required classification information be available at the defined location, in required form and within the defined period of time.

(2)Components in the Information System security policy shall be determined in the interests of

³ Regulation N. 524/2005 Coll., on Providing the Cryptographic protection of Classified Information.

providing secure operation of the Information System, which must be substitutable without breakdown of the Information System operation. Further the scope of required minimum functionality of the Information System shall be defined and those components shall be identified, the failure of which shall not affect the minimum functionality of the Information System.

(3)The planning of capacities of assets of the Information System and pursuing of capacity requirements shall be carried out in such a manner as to avoid mistakes occasioned by lack of spare capacities.

(4)A post-breakdown recovery plan shall be drawn up for the Information System. Restart of the Information System to the known security state may be carried out manually by the Information System administrator or automatically. All activities conducted to renew operation of the Information System shall be generally recorded in audit records protected from unauthorised modification or destruction.

Section 11

System-dependent security requirements based on risks analysis

(1)A risks analysis shall be conducted to determine threats to assets of the Information System.

(2)Within the frame of conducting risks analysis assets of the Information System shall be determined together with threats affecting individual assets of the Information System. In particular such threats shall be assessed, which cause the loss of functionality or security of the Information System.

(3)Subsequent to threats determination vulnerabilities shall be defined in such a manner as to define the vulnerability to each threat or sites will be found, which are affected by that threat.

(4)The result of the risk analysis conducted shall be the list of threats, which can endanger the Information System, with indication of the corresponding risk.

(5)The selection of appropriate countermeasures shall be carried out on the basis of risks analysis being conducted.

Section 12

Possibility to substitute computer security means

In justified cases the provision of some security functions of the Information System by computer security means may be substituted with increased application of personnel or administrative security means, physical security of Information Systems means or by improvement of organizational measures. The security function shall be fully implemented and the quality and the level of the security function shall be kept in the case of substitution of computer security means with substitutive security mechanism or group of mechanisms, which are designed to provide specific security function.

Section 13

Requirements for the protection of mobile and portable Information Systems

(1) In the case of mobile and portable Information Systems also those risks shall be assessed, which are related to means of transport, and in the case of portable Information Systems risks related to environments, in which these Information Systems will be used.

(2) The system of measures used for the purposes of overall protection of mobile and portable Information Systems containing components for storage of classified information, shall, in addition to other requirements stipulated by this Regulation, include the conception of this means as the carrier of classified information, which is classified at the highest classification level of classified information handled by it.

Section 14

Requirement to ensure protection against compromising electromagnetic emissions

(1) Components of the Information System handling information classified CONFIDENTIAL or above shall be safeguarded from compromising electromagnetic emissions, which could result in leakage of classified information.

(2) The level of safeguarding according to paragraph 1 is dependent on the security classification of classified information handled by the Information System, and it will be determined by security standards.

Section 15

Requirements for the security of classified information carriers

(1) All classified information carriers used during operation of the Information System shall be registered. The security classification of these information carriers shall correspond to the security mode of operation and to the highest classification of classified information stored on the carrier.

(2) Should a removable classified information carrier be intended for use in operation of a certain Information System only, also the name of the Information System in question and registration number of the information carrier shall be marked in addition to security classification. Classified information carriers intended for forwarding or release of information from the Information System shall be marked with the security classification and with other data according to the special legal regulation⁴.

(3) Classified information carriers built-in in equipment and other components enabling storage of classified information shall be recorded and marked with the security classification after their removal from the equipment in question at the latest. Equipments shall be recorded in a operational security documentation of the Information System.

(4) The TOP SECRET classification of a classified information carrier shall not be downgraded, except for the case where it has been proved that only classified information classified below or unclassified information had been stored on the medium during its hitherto lifecycle.

(5) The SECRET or CONFIDENTIAL classification of a classified information carrier may be downgraded or in the case of RESTRICTED classification declassified only if the carrier has been cleared as outlined in paragraph 6 or if it has been proved that only information classified below or unclassified information had been stored on the medium during its hitherto lifecycle.

(6) Deletion of classified information from a classified information carrier, which allows

⁴ Regulation N. 529/2005 Coll., on Administrative Security and Registries of Classified Information.

downgrading its classification level, shall be carried out in a manner that prevents from obtaining residual classified information. The procedure shall be laid down in the operational security documentation of the certified Information System.

(7) Destruction of classified information carries shall be carried out in a manner ruling out the possibility of its retrieval.

Section 16 **Requirements for access to classified information in the Information System**

(1) Only such person may be a user, security officer or Information System administrator, who has been authorised to act within the Information System by procedure laid down in the security documentation of the Information System.

(2) A user, security officer and Information System administrator shall be holders of the personnel security clearance for the security classification, which shall be determined in accordance with a security mode of operation and according to the highest security classification of classified information that may be handled by the Information System.

(3) The specific identifier shall be assigned within the Information System to the user, security officer and Information System administrator on the basis of the authorisation. In order to ensure that classified information and services of the Information System, which is full-time operated, are continuously available, the Authority may in justified cases and within the process of its certification enable more users, security officers and Information System administrators to use the specific identifier. Inseparable from this alternative shall be establishing a procedure enabling to determine which user, security officer or Information System administrator has used the identifier within a specified period of time.

(4) The authorization will be granted to a user, security officer or to Information System administrator only to the extent necessary to carry out his/her responsibilities within the Information System.

Section 17 **Requirement for responsibility for activities performed within the Information System**

(1) A user, security officer and Information System administrator shall comply with procedures laid down in the security documentation of the Information System, which shall be followed to ensure the security of the Information System.

(2) Information concerning activities of a subject of the Information System in the Information System shall be recorded in such a manner as to enable identification of any breach or any attempted breaches of security of the Information System. Records of activities of the subject of the Information System in the Information System shall be maintained for a retrospective review for a period determined in the Information System security policy.

Section 18 **Information System security administration**

(1) An appropriate system of the Information System security administration shall be established in the Information System. The role of the Information System security officer shall be established within the frame of the Information System security administration, separately from other roles within the Information System administration, unless otherwise provided herein.

(2) Other roles shall be established within the Information System security administration, if need be to provide the determined scope of activities pursuing objectives to ensure the security of the Information System, in particular the organizational structure of security officers, sites security officers, security officer for the area of communication security or security officer of the security interface of the Information Systems.

(3) The role of a security officer of the Information System includes performance of security administration of the Information System, which, in particular, consists of granting access rights, authentication and authorization information management, the Information System configuration management, management and assessment of audit records, security instructions updating, security incidents and emergencies management and drawing up reports thereon, providing technical training for users in the area of the Information System security,

control of compliance with operational security directives, as well as of other activities determined in the security documentation of the Information System.

(4) Within the frame of certification of minor Information System the Authority may allow to merge the role of the security officer with some other roles in the Information System administration.

(5) In addition to activities for providing functionality of the Information System and management of its operation, the Information System administrator shall fulfil determined activities to ensure computer and communication security of the Information System.

Section 19

Personnel security requirements in operation of the Information System

(1) Activities of a user, security officer and Information System administrator in the Information System will be allowed on the basis of their authorization for these activities, which shall be changed in the event of change in his/her role within the Information System or revoked if he/she no longer complies with conditions for access to classified information. The security officer shall maintain the list of users of the Information System.

(2) The Information System operational authority shall provide initial training of users, security officers and Information System administrators aimed at observance of measures determined in the security documentation of the Information System and correct use of the Information System. Further training shall be arranged whenever any substantial change within the Information System occurs; otherwise it shall be arranged at least annually.

Section 20

Physical security requirements of Information Systems

(1) The assets of the Information System shall be placed to a room where the Information System is physically protected to avoid unauthorised access, damage and influence. It shall be determined within the frame of certification of the Information System which components of the Information System shall be placed to the security area or facility, and the required category of the security area.

(2) Assets of the Information System shall be protected from security threats and risks resulting from the environment in which they are located.

(3) Assets of the Information System shall be located in such a manner as to prevent an unauthorised person from overlooking classified information or identification or authentication information on the user.

(4) Communication infrastructure transmitting the data or supporting services of the Information System shall be protected from the possibility of interception of classified information being transmitted and from damage.

Section 21

Requirement for security testing of the Information System

(1) Security of the Information System shall be verified prior to issuing the certificate by independent testing. No classified information may be used for the purposes of testing.

(2) Results of tests shall prove that security functions are clearly consistent with the Information System security policy. Results of tests shall be documented. Shortcomings found during testing shall be remedied and their elimination shall be verified by subsequent testing.

Section 22

Requirements for security in installation of the Information System

Installation procedure of the Information System shall be organized in a manner so as to avoid threats to its security and weakening its security functions. Components of the Information System shall be determined in the security policy of the Information System that must be installed by persons who satisfy conditions set out in the Act for access to classified information corresponding to the highest classification level to be handled in the Information System. These are components ensuring security functions of the Information System or components assessed as vulnerable in the process of installation. Other components of the Information System may be installed by persons who satisfy conditions set out in the Act for access to classified information of a lower classification level or by persons who do not satisfy

conditions for access to classified information, who were approved by a security director of the Information System user, but under continuous supervision of an officer of the Information System administration, who has been cleared for access to classified information with the highest classification level to be handled in the Information System.

Section 23

Requirements for security of the Information System being operated

(1) Security of the Information System shall be verified and assessed on an ongoing basis, with respect to actual Information System state. Any partial Information System change may be made only when bearing of this change on the Information System security is assessed and when the Authority has approved this change, save as otherwise provided in the certification report.

(2) Integrity of software and classified information shall be protected from malicious code attacks.

(3) Only such software and hardware may be used in the Information System being operated, which is in accordance with the security documentation of the Information System approved by the Authority, and with conditions of the certification report accompanying the certificate of the Information System.

(4) Backup of software and classified information shall be made in the Information System being operated. Backup of software and classified information shall be stored in such a manner so as to avoid its damage or destruction in the case of endangering the Information System or to avoid misuse resulting in a breach of confidentiality of classified information.

(5) Maintenance work in the Information System being operated shall be organized in such a manner so as to avoid endangering its security. All classified information shall be deleted on classified information carriers, which are accessible during maintenance

work and remote diagnostics shall be protected from misuse.

(6) Maintenance of Information System components providing security functions of the Information System or directly affecting security of the Information System shall be carried out by persons who satisfy the conditions set out in the Act for access to classified information corresponding to the highest classification level to be handled in the Information System. Such components shall be determined in the operational security documentation of the Information System. Maintenance of other components of the Information System may be carried out by persons who satisfy the conditions set out in the Act for access to classified information of a lower classification level or by persons who were approved by a security director of the Information System user, but under continuous supervision of an officer of the Information System administration, who has been cleared for access to classified information with the highest classification level to be handled in the Information System.

(7) Evaluation of audit records shall be undertaken in the Information System being operated within deadlines laid down in the security documentation of the Information System and in emergency without delay. Audit records shall be archived for a period determined in the security documentation of the Information System and protected from its modification or destruction.

(8) In order to enable resolving any emergency situation of the Information System being operated such measures shall be laid down in the security documentation of the Information System, which are aimed at its bringing into the state consistent with the security documentation of the Information System. Basic types of emergencies shall be laid down in the security documentation of the Information System, which can arise according to the risks analysis, and following actions shall be specified for each type of emergency

- a) the action to be undertaken immediately after the emergency situation has arisen, aimed at damage minimizing and at obtaining information that is necessary for assessment of reasons and mechanisms of occurrence of the emergency; and
- b) the action to be undertaken after the emergency situation has arisen, which is aimed at elimination of consequences of the emergency

including setting out personal responsibilities for individual tasks.

(9) For the case of failure or malfunction of software or hardware the following procedures shall be laid down in the security documentation of the Information System

- a) backup of the Information System and storage of backup media;
- b) providing maintenance work;
- c) providing emergency mode of operation of the Information System and listing minimum functions, which shall be maintained; and
- d) recovery of functionality and restoring of the Information System to the known secure state.

(10) Prior to final termination of operation of the Information System carriers of classified information, which has been handled by the Information System, shall be removed or destroyed.

CHAPTER II INFORMATION SYSTEMS CERTIFICATION

Section 24 Application for the Information System certification and the method and conditions of its carrying out

(1) An application for the Information System certification shall contain the following

- a) identification of the applicant by
 1. the name of the company or the name, location and registration number should the applicant be a legal person;
 2. the name of the company or the name and surname or any differentiating affix, permanent residence address and the place of business activity if different from the permanent residence, date of birth and identification number should the applicant be a natural person pursuing business; or
 3. the name, location, registration number and the name and surname of the responsible person in the case of the State body;

- b) the name and surname of the contact officer of the applicant and the contact address;
- c) brief description of the purpose and extent of the Information System;
- d) security classification of classified information to be handled in the Information System;
- e) determination of security mode of operation of the Information System; and
- f) identification of a provider of the Information System or of its components affecting security of the Information System, according to subparagraph (a) bullets 1. or 2., and security classification for which the provider has been issued with the facility security clearance.

(2) The following source materials shall be submitted by the applicant for the purpose of carrying out certification of the Information System

- a) the security policy of the Information System and results of the risks analysis;
- b) the security proposal of the Information System;
- c) the set of security tests of the Information System, their description and description of test results;
- d) the security operational documentation of the Information System;
- e) the description of security of the development environment; and
- f) other materials necessary for the Information System certification resulting from the Information System specification.

(3) Should the Intelligence Service application for the Information System certification, it will state only necessary data in the application according to paragraph 1 and in materials according to paragraph 2, which allow the Information System certification by the Authority.

(4) Also results of partial tasks in evaluation of some components of the Information System and in evaluation of individual areas of security as outlined in S. 3 par. 1, carried out by the State body or facility under contract for providing services, which has been concluded with the Authority, may be submitted by an applicant as a documentation for the Information System certification.

(5) In the conduct of Information System certification the capability of set of measures proposed to attain the Information System security according to S. 3 shall be assessed, as well as validity

and completeness of the security documentation of the Information System and correctness of implementation of the proposed set of measures within the Information System in question.

(6)The Information System certification shall be based on assessment of documents submitted by an applicant and additional testing. Additional tests shall be carried out by the Authority in the operational environment of the Information System being evaluated in the presence of the applicant and, if necessary, of the provider.

(7)The Information System certification may be carried out continuously upon completion of individual stages of the Information System construction or after it has been completed.

(8)Whenever a change occurs according to S. 25(d) in the Information System that has been certified and approved to the live activation, the additional assessment of the Information System shall be carried out to the extent necessary for evaluation of changes made. In the case of additional assessment of the Information System the procedure will be similar to that in the case of certification of the Information System.

(9)The format of the Information System certificate is shown in Annex 1 to this Regulation.

Section 25

Certification report of the Information System

The certification report shall contain the following

- a) brief description of the Information System;
- b) operational conditions of the Information System;
- c) identification of possible acceptable risks specific to the operation of the Information System; and
- d) types of changes of the Information System requiring carrying out additional assessment of the Information System.

Section 26

Application for re-certification of the Information System and the method of its carrying out

(1)An application for re-certification of the Information System shall contain the following

- a) identification of the applicant according to S. 24 1(a);
- b) complete identification of the Information System certificate issued containing its holder, registration number, date of issuance and validity period;
- c) identification of the Information System containing its name, version mark and security classification of classified information for which its capability has been approved; and
- d) the name and surname of the contact officer of the applicant and the contact address.

(2)If the applicant proves that the Information System will be operated under conditions laid down in the certification report on the expiry date of the current certificate and neither the applicant or the Authority identified new risks for the Information System, the Authority will issue the certificate on the basis of current security documentation of the Information System and on the basis of the control of the Information System security conducted.

(3)If a user proposes a change in the security policy of the Information System on the expiry date of the current certificate or if new risks for the Information System has been identified, the Authority shall ask amending or adjusting of corresponding parts of the documentation and carry out additional assessment of the Information System to the extent determined by the Authority. If the Information System complies with determined security conditions the Authority will issue the certificate.

(4)If changes proposed in the security policy of the Information System are essential for overall security of the Information System, the Authority shall pursue the same line as with the new certification.

PART THREE COMMUNICATION SYSTEM

Section 27

Elements of the Communication System security project

(1) The security policy of the Communication System shall set out the manner in which

confidentiality, integrity and availability of classified information will be provided and specify responsibility of an user for his activities within the Communication System in question.

(2)The security policy of the Communication System contains body of principles and requirements in the area of personnel, administrative, physical and communication security, which have been determined depending on the security classification of classified information being transmitted, on results of risks analysis of the Communication System and on principles and conditions of operation of the cryptographic device provided for in the certification report of the cryptographic device.

(3)Organizational measures and operational procedures governing operation of the Communication System shall contain the following

- a) the manner in which the cryptographic protection will be implemented in accordance with the certification report of the cryptographic device;
- b) the required structure of the Communication System administration; and
- c) organizational measures and principles of operational procedures, which, when fulfilled and carried out, ensure that classified information transmitted within the Communication System will be protected.

(4)Operational instructions for the Communication System administration and operational instructions of the Communication System user shall be prepared separately on the basis of the Communication System security policy and on the basis of organizational measures and operational procedures governing operation of the Communication System. These instructions shall contain specific operational procedures to provide for the security administration of the Communication System and performance of the cryptographic protection and to determine responsibilities of the Communication System administration staff, cryptographic protection staff and users to ensure that classified information will be protected accordingly.

Section 28

Application for approval of the Communication System security project

(1)The State body or facility that will operate the Communication System shall submit an application

for approval of the Communication System security project.

(2)The application according to paragraph 1 shall contain

- a) the identification of the applicant according to S. 24 par. 1(a);
- b) the name and surname of the contact officer and the contact address;
- c) should the applicant be a facility, the level and number of the facility security clearance;
- d) the name and brief description of the purpose and scope of the Communication System including determination of its routine operational functions;
- e) security classification of classified information to be handled by the Communication System; and
- f) identification of a provider of components of the Communication System affecting security of the Communication System, according to S. 24 par. 1 sub-paragraph (a) bullets 1. or 2., and security classification for which the facility has been issued with the facility security clearance.

(3)During the approval process parts of the Communication System security project according to S. 27 par. 2 will be enclosed to the application according to par. 2.

(4)Should the Intelligence Service request for the approval of the Communication System security project, it will state only necessary data in the application according to paragraph 2 and in documents according to paragraph 3, allowing the approval of the Communication System security project by the Authority.

Section 29

Method and conditions for approval of the Communication System security project

(1)Within the framework of the approval process of the Communication System security project the applicability of the body of principles and requirements in the area of personnel, administration, physical and communication security according to S. 27 par 2 shall be assessed, and applicability of organizational measures and operational procedures with respect to the Communication System operation according to S. 27 par. 3, which have been proposed to provide security of the Communication System, as well as correctness and completeness of operational instructions according to S. 27 par. 4.

(2) Approval of the Communication System security project shall be based on assessment of documents submitted by an applicant and on the check of implementation of the Communication System security project made by the Authority in the operational environment of the Communication System being approved.

(3) Approving of the Communication System security project may be carried out continuously upon completion of individual stages of the Communication System construction or after it has been completed, according to requirements of an applicant.

(4) If it has been determined during the approval process of the Communication System security project that the Communication System being evaluated has the capability to handle classified information, the applicant shall receive the written approval of the Communication System security project.

(5) Whenever significant changes occur in the Communication System affecting overall security of this Communication System, the additional assessment of the Communication System shall be carried out to the extent necessary for evaluation of changes made. In the case of additional assessment of the Communication System the procedure will be similar to that in the case of approval of the Communication System security project.

PART FOUR COMPROMISING ELECTROMAGNETIC EMISSIONS

CHAPTER I ELECTRIC AND ELECTRONIC DEVICE, SECURITY AREA OR FACILITY

Section 30 Application for verification of capability of electrical and electronic device, security area or facility

(1) An application for verification of capability of electrical and electronic device, security area or facility shall contain the following

- a) the identification of the applicant according to S. 24 par. 1(a);
- b) the name and surname of the contact officer and the contact address;
- c) the identification of the electrical or electronic device, security area or facility, the capability of which shall be verified;
- d) security classification of classified information to be processed in the electrical or electronic device, security area or facility.

(2) The report on results of evaluation of capability of electrical or electronic device, security area or facility to ensure the protection from leakage of classified information through compromising electromagnetic emissions may be enclosed in the application, which has been carried out by the State body or facility under contract for providing services concluded with the Authority.

(3) Conditions of evaluation and application of electrical and electronic device, security area or facility for the protection of classified information from leakage of classified information through compromising electromagnetic emissions shall be determined by the Authority in security standards.

Section 31 Method of evaluation of capability of electrical and electronic device, security area or facility

(1) Evaluation of capability of electrical and electronic device with respect to leakage of classified information through compromising electromagnetic emissions shall be carried out by measurement of levels of the radiated electromagnetic field and checking of values measured against the security standards.

(2) Evaluation of capability of the security area or facility to protect classified information from its leakage through compromising electromagnetic emissions shall be carried out by measurement of its attenuation characteristics and checking of values measured against the security standards.

(3) Should any discrepancy be discovered during the process of evaluation of capability of electrical and electronic device, security area or facility, the Authority shall call on the applicant to remedy it.

(4) The Authority shall draw up the report on the course and results of evaluation of capability of

electrical and electronic device, security area or facility to provide the protection from leakage of classified information through compromising electromagnetic emissions and the applicant shall be notified in writing of the result.

CHAPTER I SHIELDED CHAMBER

Section 32

A shielded chamber certified by the Authority may be used, inter alia, for the protection of classified information from its leakage through compromising electromagnetic emissions. Conditions of evaluation of the shielded chamber for the protection of classified information shall be determined by the Authority in security standards.

Certification of the shielded chamber

Section 33 Application for certification of the shielded chamber

(1) An application for certification of the shielded chamber shall contain the following

- a) the identification of the applicant according to S. 24 par. 1(a);
- b) the name and surname of the contact officer and the contact address;
- c) should the applicant be a facility, the level and number of the facility security clearance;
- d) the identification and location of the shielded chamber; and
- e) the identification of the producer of the shielded chamber, according to S. 24 par. 1 sub-paragraph (a) bullets 1. or 2.

(2) The report on results of evaluation of the shielded chamber may be enclosed in the request, which has been carried out by the State body or facility under contract for providing services concluded with the Authority. The result of evaluation provided for in the enclosed report shall not extend beyond six months from the date of submission of the application for certification of the shielded chamber.

Section 34

Method and conditions for carrying out certification of the shielded chamber

(1) Certification of the shielded chamber shall be carried out by measurement of attenuation characteristics of the shielded chamber and checking of values measured against the security standards. Measurement of the shielded chamber shall be carried out with the participation of the applicant and, where appropriate, also the provider of the shielded chamber.

(2) The Authority shall draw up the report on the course and partial results of the shielded chamber certification.

(3) The format of the certificate of the shielded chamber is shown in Annex 2 to this regulation.

Section 35 Certification report of the shielded chamber

The certification report of the shielded chamber shall contain the following

- a) brief description of the shielded chamber, its location and purpose of its use;
- b) conditions for the shielded chamber operation; and
- c) types of changes requiring re-certification of the shielded chamber.

Section 36 Application for re-certification of the shielded chamber and the method used

(1) An application for re-certification shall contain the following

- a) the identification of the applicant according to S. 24 par. 1(a);
- b) complete identification of the shielded chamber certificate issued, which contains its holder, registration number, date of issuance and validity period;
- c) the identification of the certified shielded chamber containing its name, type designation, variant construction and location; and
- d) the name and surname of the contact officer and the contact address.

(2) The report on results of evaluation of the shielded chamber may be enclosed in the request,

which has been carried out by the State body or facility under contract for providing services concluded with the Authority, according to S. 33 par. 2.

(3) If the applicant proves that no changes in conditions occur on the expiry date of the current certificate of the shielded chamber, which are determining for the validity of the certificate issued, the Authority will issue the certificate.

(4) If the applicant cannot prove facts outlined in paragraph 3 on the expiry date of the shielded chamber certificate, the Authority will conduct additional evaluation of the shielded chamber, and if capability of the shielded chamber to protect classified information is verified, it will issue the certificate. If substantial changes of operational conditions have been made, the procedure will be the same as in the case of new certification.

PART FIVE ELEMENTS OF THE APPLICATION OF THE STATE BODY OR FACILITY FOR MAKING THE CONTRACT FOR PROVIDING SERVICES

Section 37

An application for making the contract for providing services shall contain the following

- a) the identification of the applicant according to S. 24 par. 1(a);
- b) should the applicant be a facility, the level and number of the facility security clearance;
- c) the name and surname of the contact officer and the contact address;
- d) the identification of the specialized site of the applicant (subject-matter of activities and detailed specification of location of the site being enquired, the name and surname of the contact officer and the contact address);
- e) the specification of activities to be conducted according to the contract;
- f) the personnel conditions of the site to perform required activities (the name, surname and qualification of the head of the specialized site, names and surnames of other specialists of the site and their qualification);

- g) the statement of the responsible person concerning the physical, personnel and administrative security that is provided for the specialized site;
- h) the level and registration number of the Information System certificate, should the use of the certified Information System be necessary for activities according to the contract; and
- i) the availability of technical means within the specialized site, which is necessary for conducting activities according to the contract.

PART SIX CONDITIONS FOR SECURE OPERATION OF COPYING MACHINES, DISPLAY DEVICES OR MEMORY TYPEWRITERS

Section 38

(1) The secure operation of copying machines, display devices or memory typewriters that are not parts of Information or Communication Systems can be achieved by enforcement of the set of measures from the following areas

- a) the personnel security;
- b) the physical security;
- c) the administration security and organizational measures; and
- d) the protection of classified information from its leakage through compromising electromagnetic emissions.

(2) Copying machines, display devices or memory typewriters that are used for the processing of information classified CONFIDENTIAL and above shall be secured against leakage of classified information through compromising electromagnetic emissions. In verifying of capability of copying machines, display devices or memory typewriters to protect classified information from its leakage

through compromising electromagnetic emissions the procedure shall be in accordance with S. 31.

(3) Copying machines, display devices or memory typewriters shall be placed in the area where their physical protection is provided against unauthorised access, damage and influence. This area shall be determined by defined protection elements with corresponding access controls and security barriers. According to the character of equipment it shall be determined on the basis of risks analysis, whether it shall be placed in the security area or in the facility, and the required category of the security area. The risks analysis shall determine the likelihood of vulnerabilities of the equipment being successfully exploited by a threat and an assessment of consequences.

(4) Copying machines, display devices or memory typewriters shall be physically protected against security threats and environment risks.

(5) Copying machines, display devices or memory typewriters shall be placed in such a manner as to counter the risk from unauthorised overlooking of classified information.

(6) The information shall be marked on the copying machines and display devices with fixed classified information carriers or other components enabling storage of classified information, and on memory typewriters, indicating the security classification of classified information stored on these carriers, components and in memories. This information may be marked on the label fixed to the equipment, determined in security operating instructions or otherwise indicated. Fixed classified information carriers and other components for storage of classified information shall be recorded and marked with the security classification after their removal from the device at the latest.

(7) Maintenance of copying machines, display devices or memory typewriters shall be organized in such a manner as to avoid endangering security of classified information. Classified information stored on classified information carriers and memories accessible during maintenance work shall be erased.

Section 39

This Regulation shall come into force on 1 January 2006.

Director

Signed

Mgr. Mareš

PART SEVEN COMING INTO FORCE

NATIONAL SECURITY AUTHORITY

P.O.Box 49
150 06 Prague 56

The National Security Authority issues according to S. 46 of the Act N. 412/2005 Coll., on the Protection of Classified information

CERTIFICATE
of the Information System

Registration number:

.....
(name, version)

Holder of the certificate:

Location/permanent residence/address:

Registration number/Personal Identity Number:

This certificate confirms verification and approval of capability of the Information System to handle classified information classified up to and including

Valid from:

Date of expiry:

Stamp

Signature of authorised representative

Date of issuance:

Annexes:

NATIONAL SECURITY AUTHORITY

P.O.Box 49
150 06 Prague 56

The National Security Authority issues according to S. 46 of the Act N. 412/2005 Coll., on the Protection of Classified information

CERTIFICATE
of the shielded chamber

Registration number:

.....
(name, type designation)

Holder of the certificate:

Location/permanent residence/address:

Registration number/Personal Identity Number:

Producer of the shielded chamber:

Location/permanent residence address:

Registration number/Personal Identity Number:

This certificate confirms capability of the shielded chamber to protect classified information from its leakage through compromising electromagnetic emissions, classified up to and including

.....

Valid from:

Date of expiry:

Stamp

Signature of authorised representative

Date of issuance:

Annexes: