UNOFFICIAL TRANSLATION

ROMANIA

GOVERNMENT OF ROMANIA

GOVERNMENT DECISION no. 353/2002 on

NORMS ON THE PROTECTION OF NATO CLASSIFIED INFORMATION IN ROMANIA

BUCHAREST
- 2002 -

A. FUNDAMENTALS

1. In its capacity of candidate to accession and partner state to the North Atlantic Cooperation Council, Romania signed, on 8th July1994, the Security Agreement with the North Atlantic Treaty Organization, hereinafter NATO, and on 10th September 1994, the Code of Conduct.

2. By signing the above-mentioned documents, Romania committed itself to "protect and safeguard classified information and material" of the Alliance and its members, according to the standards provided in the document "Security within the North-Atlantic Treaty Organization – C-M (55) 15 (Final)" and the national legislation.

3. In compliance with the obligations assumed by Romania, the National Security Authority, hereinafter NSA, was established by Government Decree no. 864/10th October 2000, and was entrusted with regulation, authorization and control tasks, in compliance with the minimum standards for the protection of NATO classified information.

4. The National Security Authority (NSA) is the national point of contact with the NATO Office of Security (NOS) and with other similar security structures of the North Atlantic Alliance. NSA ensures the unitary co-ordination and implementation of the activity for the protection of NATO classified information in Romania.

5. NSA exerts its tasks in the following areas: physical security, personnel security, document security, protection of information stored within the systems for automatic data processing, hereinafter INFOSEC, industrial security, as well as other areas involving the protection of NATO classified information. To this end, NSA draws up domestic instructions and procedures, in strict observance of the national legislation and NATO relevant standards.

6. The institutions responsible for the protection of NATO classified information are the following: Romanian Intelligence Service, Foreign Intelligence Service, Ministry of National Defense, i.e. Defense Intelligence General Directorate, and Ministry of Foreign Affairs. At the same time, Special Telecommunications Service, Ministry of Interior and Guard and Protection Service shall fulfill specific tasks according to their legal competence.

B. DEFINITIONS

7***. Information*** means knowledge that can be communicated in any form.

8. ***Classified information*** means information or material determined to require protection against unauthorized disclosure, which has been so designated by the security classification.

9***. Material*** includes documents and any item of machinery or equipment, or weapons, either manufactured or in the process of manufacture.

10. ***NATO classified information*** means all classified information, military, political and economic, circulated within NATO, whether such information originates in NATO commands and agencies, or is received from member nations or from other international organizations.

11. ***Document*** means any recorded information, regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies and ink ribbons, or reproductions by any means of process, and sound, voice, magnetic or electronic, or optical or video recordings, in any form, and portable ADP, equipment with resident computer storage media, and removable computer storage media.

12***. NATO classified document*** means any document containing NATO classified information.

13. ***Security of NATO classified documents*** means all procedures, instructions and measures for the management and control of NATO classified documents.

14***. Management of NATO classified information*** means all activities of receiving, recording, drawing up, consultation, verification, dissemination, transmission, transport, copying, destruction, inventory and archiving of NATO classified information.

15. ***Control of NATO classified information*** means all activities that verify how NATO classified information is managed.

C. ACCESS TO NATO CLASSIFIED INFORMATION

16. Access to NATO classified information is granted on the basis of the security clearance certificate, in strict observance of the need-to-know principle.

17. According to the Government Decree 864/10.10.2000, NSA issues the security clearance certificates attesting the right of access to NATO classified information and documents.

18. Two types of security clearance certificates are issued, as follows:
- Type A: NATO Personnel Security Clearance Certificate – granting access to NATO classified information, with a three-year period of validity;
- Type B: Certificate of Security Clearance – granting to an individual the right to participate in activities organized by the Alliance, where NATO classified information is circulated and for which the Alliance requests the issuance of such a document. The certificate is valid only for the period the activity is carried out. A Type B certificate of security clearance requires previous issuance of a Type A personnel security clearance certificate.

19. The level of access granted by the security clearance certificate shall be similar to the classification level of the information to which the individual needs access in fulfilling its duties.

20. Access to NATO classified information based on the security clearance certificate shall observe the need-to-know principle, i.e. no person is entitled solely by virtue of rank, position or personnel security clearance certificate to have access to NATO classified information. The number of individuals having access to NATO classified information and documents shall be limited to those whose professional duties require access to such information.

21. The individuals who have been issued security clearance certificates and are going to be granted access to NATO classified information will be briefed by the Security Officer (SO) of the organization on the norms and regulations for the protection of such information. The individuals will pledge, in writing, to safeguard NATO classified information, and to comply with the provisions of the relevant regulations/security plans, in fulfilling their duties.

D. NATIONAL REGISTRY SYSTEM (NRS)

22. ***Institutional structure*** means any ministry, central body, organization, authority agencies, economic units that handle/will handle NATO classified information.

23. ***Component of the National Registry System (CNRS)*** is that component of an institutional structure responsible for the management and consultation of NATO classified information. These are: the Central Registry, external registries, internal registries, sub-registries and control points.

24. **The *National Registry System*** consists of all CNRSs.

25. The regulations on physical security, personnel security, document security, INFOSEC and industrial security are unitary implemented within the NRS, in order to ensure the appropriate framework for the management of NATO classified information, in accordance with NATO security standards.

26. Each institutional structure (military or civilian) which handles NATO classified information shall establish its own CNRS. The organizational form of this CNRS shall depend on the amount and classification level of the handled information, and shall be consistent with the existing administrative structure.

27. The ***Central Registry*** is that CNRS established and functioning within the NSA. It is responsible for the management and control of all NATO classified information, at national level.

28. An ***External Registry*** is that CNRS functioning outside the country, subordinated to the Central Registry, responsible for the management of NATO classified information received/released from/to NATO and the other security structures of the Alliance.

29. An ***Internal Registry*** is that CNRS responsible for the management and control of NATO classified information, at the level of an institutional structure.

30. A ***Sub-registry*** is that CNRS subordinated to a Registry, responsible for the management and control of NATO classified information, at departmental level.

31. A ***Control Point*** is that CNRS exerting solely accountability, consultation, dissemination, storage and control tasks of NATO classified information.

32. A CNRS shall be organized in relation to the amount and classification level of NATO classified information it manages, as well as to the functional tasks it will fulfill. A CNRS is composed of:

A. The Document Section, with:
- a recording section, and
- a dissemination section;

B. The Courier Section.

33. The Document Section has the following main tasks:
- to receive, record, keep record of the drawing up and consultation, check, transmit, transport, copy, destroy, make inventory, archive and control NATO classified information;
- to disseminate NATO classified information – collection, checking, wrapping, and dispatching.

34. The Courier Section has the following main tasks:
- to collect, check, and transport NATO classified documents, in accordance with the national regulations on transport of national classified documents with equivalent classification level, observing NATO minimum security standards.

35. Each CNRS shall establish a Document Section. The Courier Section could be included in/ensured by/ the institutional structure it belongs to.

36. Tasks of the Central Registry:
a. to co-ordinate the activity of all subordinated CNRS;
b. to implement the specific methodologies issued by the NSA within its own structure, to transmit them to all subordinated CNRS and to ensure they are properly implemented;
c. to manage NATO classified information*;*
d. to ensure the organization and functioning of the NATO classified information archive, at national level;
e. to make the annual inventory of all documents it manages and to centralize the results of the inventories carried out in all CNRS*;*
f. to manage all original Type A personnel security clearance certificates issued by the NSA;
g. to keep record of all subordinated CNRS;

h. to control periodically how NATO classified information is managed within the subordinated CNRS;
i. to train and brief its own personnel.

37. Tasks of the External Registry:
a. to implement the specific methodologies issued by the NSA within its own structure, to transmit them to all subordinated CNRS and to ensure they are properly implemented;
b. to receive/transmit classified information from/to NATO and other security structures of the Alliance;
c. to manage NATO classified information received from / transmitted to/ the Central Registry;
d. to ensure the organization and functioning of its own NATO classified information archive;
e. to make the annual inventory of all documents it manages and to centralize the results of the inventories carried out in all subordinated CNRS*;*
f. to manage all original Type B certificates of security clearance issued to the individuals employed by the institutional structure;
g. to keep record of all subordinated CNRS;
h. to control periodically how NATO classified information is managed within the subordinated CNRS and centralize the results;
i. to train and brief its own personnel;
j. to support activities relating to the protection of NATO classified information organized by NATO;
k. to transmit to NOS documents related to the protection of NATO classified information originating from the NSA.

38. Tasks of the Internal Registry**:**
a. to co-ordinate the activity of all subordinated CNRS, i.e. Sub-registries or Control Points;
b. to implement the specific methodologies issued by the NSA within its own structure, to transmit them to all subordinated CNRS and to ensure they are properly implemented;
c. to manage NATO classified information, to ensure the information flow from/to the subordinated CNRS, as well as to transmit national documents to the Central Registry *;*
d. to ensure the organization and functioning of the NATO classified information archive, at the level of the institutional structure it belongs to;
e. to make the annual inventory of all documents it manages and to centralize the results of the inventories carried out in all subordinated CNRS*;*
f. to manage all original security clearance certificates (Type A and B) issued by the NSA, for the personnel of its own structure

and to keep an up-to-date list of all individuals in the CNSR who have access to NATO classified information;
g. to keep record of all subordinated CNRS;
h. to control periodically how NATO classified information is managed within the subordinated CNRS;
i. to train and brief its own personnel, as well as the personnel of the subordinated sub-registries and control points.

39. Tasks of the Sub-registry:
a. to co-ordinate the activity of all subordinated CNRS, i.e. Control Points;
b. to implement the specific methodologies issued by the NSA within its own structure;
c. to manage NATO classified information, to ensure the information flow from/to the subordinated CNRS, as well as to transmit national documents to the Registry*;*
d. to ensure the organization and functioning of its own NATO classified information archive;
e. to make the annual inventory of all documents it manages and to centralize the results of the inventories carried out in all subordinated CNRS*;*
f. to manage all original security clearance certificates (Type A and B) issued by the NSA, for the personnel in its area of competence;
g. to keep record of all subordinated CNRS;
h. to control periodically how NATO classified information is managed within the subordinated CNRS;
i. to train and brief its own personnel, as well as the personnel of the subordinated control points.

40. Tasks of the Control Points:
a. to implement the specific methodologies issued by the NSA and transmitted through CNRS to which it is subordinated.
b. to manage all original security clearance certificates (Type A and B) issued by the NSA.
c. to ensure the organization and functioning of its own NATO classified information archive;
d. to make the annual inventory of all documents it manages;
e. to ensure the recording, consultation, dissemination, control and storage of NATO classified information and to transmit national documents to the hierarchically superior CNRS.

41. NATO classified documents are managed exclusively within the National Registry System.

42. The documents received by the External Registry from NATO, SHAPE or other security structures of the Alliance are managed in accordance with the procedures issued by the NSA and then, they are sent to the Central Registry which is the only channel of transmitting/receiving NATO classified information to/from NATO.

43. The Central Registry will transmit/receive NATO classified information to/from directly subordinated CNRS, in accordance with the existing procedures. In their turn, these CNRS shall transmit/receive the information to/from the subordinated CNRS, observing the same procedures.

44. The Central Registry shall transmit the classified documents to NATO, through the External Registry, in accordance with the existing procedures.

45. Each institutional structure, which, in carrying out its activity, handles/will handle NATO classified information, shall establish its own CNRS.

46. A CNRS shall be established based on a unitary procedure that is finalized with the issuance of an Authorization of Organization and Functioning. This document is issued by the NSA and attests that all security standards on the protection of NATO classified information are met.

47. NSA, through the Central Registry, keeps record of all CNRS, as well as the accountability of all documents referring to their establishment / transformation/disestablishment and shall conduct periodic inspection on the way the security conditions are fulfilled.

48. Each institutional structure shall keep an up-to-date record of all establishments/transformations/disestablishments of the subordinated CNRS.

49. NSA shall submit to the NOS, at the annual inspections, the up-to-date listing of all CNRS at national level and shall inform, whenever necessary, the national institutions with responsibilities for the protection of classified information on the relevant activity in the field.

50. In case the tasks of a CNRS are changed, i.e. increased or diminished, it is necessary that the CNRS be transformed.

51. The transformation of a CNRS shall be done at the request of the institution, with the approval of the NSA, and shall become fact with the issuance of a new Authorization of Organization and Functioning.

52. A CNRS shall be disestablished when its functioning is no longer justified, and shall be done upon written request of the institution.

53. NSA will assess the request and, subsequently, will approve the disestablishment.

54. Once a year or whenever necessary, NSA shall inspect the Central Registry, based on written inspection schedule. The inspection results shall be written in an Inspection Report.

55. The members of the inspection team shall be designated by the NSA Coordination Board.

56. The Inspection Report will be assessed by the NSA Coordination Board. The conclusions will be written in a Decision. The Coordination Board shall establish the necessary measures to be further taken and deadlines to ameliorate the deficiencies resulted form the control.

57. In case of security incidents, NSA shall immediately inform the NOS and, at national level, the institutions responsible for the protection of classified information. NSA shall also inform on the measures taken to work out the incident.

58. Annually or whenever necessary, NSA, through the Central Registry, shall inspect the internal/external registries and shall draft the Inspection Report that will be submitted to the Coordination Board.

59. The members of the inspection team will be designated by the NSA Coordination Board.

60. The Inspection report shall be drafted within seven days from the date of the inspection.

61. The conclusions and recommendations provided in the Inspection Report shall be submitted to the Coordination Board for analysis and approval. Within seven days, the NSA Technical Secretariat shall inform the management of the institutional structure on the control results, the recommendations of the Coordination Board and the measures that should be taken to work out the deficiencies.

62. The Inspection Report, and the measures/recommendations, will be kept at the Central Registry and will be considered record documents; a copy will be sent to the respective registry.

63. In case of security incidents, NSA shall immediately inform NOS and, at national level, the institutions responsible for the protection of classified

information. NSA will also inform on the measures taken to work out the incident.

64. Annually or whenever necessary, the institutional structures that hold sub-registries shall inspect, through the internal registries, all the subordinated sub-registries and shall draft the Inspection Report.

65. The members of the inspection team shall be designated by the management of the organization, from the personnel of the internal registry to which it is directly subordinated.

66. The conclusions and recommendations included in the Inspection Report shall be assessed and approved by the management of the Internal Registry. The inspection results and the measures taken shall be sent to the management of the institution within 7(seven) days from the inspection date.

67. The Inspection Report together with the measures/recommendations shall be kept at the CSNR to which the respective sub-registry is subordinated, and shall represent accountability documents; a copy of them shall be sent to the inspected sub-registry.

68. In case of security incidents, NSA shall immediately inform NOS and, at national level, the institutions responsible for the protection of classified information. NSA will also inform on the measures taken to work out the incident.

69. Annually or whenever necessary, the CNRS shall inspect the subordinated Control Point and shall draft the Inspection Report.

70. The members of the inspection team will be designated by the management of the CNRS to which the Control Point is subordinated.

71. The conclusions and recommendations included in the Inspection Report shall be assessed and approved by the management of the CNRS. The inspection results shall be sent to the management of the institution within 7(seven) days from the inspection date.

72. The Inspection Report together with the measures / recommendations shall be kept at the CSNR to which that Control Point is subordinated, and shall represent accountability documents; a copy of them shall be sent to the inspected Control Point.

73. In case of security incidents, NSA shall immediately inform NOS and, at national level, the institutions responsible for the protection of classified

information. NSA will also inform on the measures taken to work out the incident.

E. PHYSICAL SECURITY

74. ***Physical security*** means all regulations, norms and measures meant to prevent unauthorized access to NATO classified information, as well as any situations, circumstances or deeds that could endanger or compromise the security and integrity of this information.

75. NSA is responsible for the issuance of the relevant regulations, the designing of the protection measures for its own location and their correct implementation.

76. The managers of the institution shall ensure the implementation and observance of the physical protection measures for NATO classified information, by appointing a security structure/officer.

77. The levels of physical protection are established depending on the following:

a. classification level of the information;
b. amount and physical frame of NATO classified information;
c. level of access granted by the security clearance certificate, with the observance of the need-to-know principle;
d. situation in the location area of the objective.

78. The term *objective* defines all security areas where NATO classified information is stored.

79. There are three classes of security areas defined, organized and administered according to the following criteria:

a) Class I Security Area means that any person in this area has access to NATO classified information. NATO classified information up to SECRET can be handled in this area. Such an area requires:

1) a clearly defined and protected perimeter, with all entrances and exits controlled;
2) control systems to allow access only for appropriately cleared and specially authorized personnel;
3) indication of the class and security level of the information within.

b) Class II Security Area means that NATO classified information within this area is managed by specific protective measures against

unauthorized access. NATO classified information up to CONFIDENTIAL can be managed in this area. Such an area requires:

1) clearly defined and protected perimeter with all entrances and exits controlled;
2) control systems to allow access only for cleared and authorized personnel. For all the other individuals, escort and surveillance rules must be in place to prevent unauthorized access.

c) Administrative Area

Around Class I and Class II security area, an administrative area may be established, with visible perimeter. Within this area, access of personnel and vehicles shall be controlled. Only NATO RESTRICTED information can be managed in the administrative area.

80. The premises where there is no 24-hour work shall be checked at the end of working hours to verify if NATO classified information is appropriately protected.

81. The access in Class I and Class II Security Areas will be checked by means of an access permit or an electronic identification control system. A control system for visitors will be established in order to prevent unauthorized access to NATO classified information.

82. The access permit shall not clearly display the identity of the originating institution or the location to which the holder has access. Entrance and exit control may be supported by an automated identification system, which shall not be a substitute for the guard and security system.

83. On the spot or upon order, at the entrance or exit of Class I and Class II Security Area, personal luggage shall be checked (including bags, parcels, and other containers that can be used for the transportation of NATO classified information.

84. The personnel ensuring the guard and security system of the security areas and NATO classified information managed within the objective shall be issued a security clearance certificate and shall be permanently briefed on how to carry out its relevant tasks

85. On off-hours and non-working days, perimeter patrols shall be organized at intervals stipulated in the instructions drafted on the basis of the Security Plan of the building.

86. In order to make the guard and security systems more efficient, access control systems shall be used (CCTV, alarm and visual inspection systems). An intervention force for emergency situations shall be

established. The reaction time of the intervention force shall be periodically tested.

87. When alarm systems, CCTV or other devices for the surveillance of the security areas or protection of NATO classified information are used, a reserve power source will be used.

88. NATO classified information shall be stored in special containers, as follows:

- Class A: safes (cipher containers) approved by the NSA, for the storage of NATO TOP SECRET information;
- Class B: metallic containers, with cipher, for the storage of NATO SECRET and NATO CONFIDENTIAL information;
- Class C: office furniture appropriate only for the storage of NATO RESTRICTED information.

89. In emergency cases, if NATO classified information must be evacuated metallic cases shall be used.

90. The locks of the containers in which NATO classified information is stored shall not be taken out of the building. There are three groups of locks, such as:

- Group A: approved by the NSA, for Class A containers;
- Group B: for Class B containers;
- Group C: only for Class C office furniture;

91. The combinations of the container locks shall be known only by authorized personnel.

92. During off-hours, the personnel of the guard and security system shall keep, in sealed boxes, the keys from offices and containers where NATO classified information is stored. These keys shall be used for intervention in case of emergency. The boxes shall be delivered / received against signature in a special registry.

93. The spare keys and combinations of the locks shall be kept in sealed envelopes by the chief of the security structure/officer. Each combination shall be kept in a separate envelope. The keys and envelopes shall be protected according to the classification level of the information they give access to.

94. Knowledge of the combinations shall be restricted to a minimum number of personnel. The keys and combinations will be changed as follows:

a) whenever a change of personnel handling them occurs;
b) in case of a security incident or security risk;

c) at regular intervals, preferably once in 6 months (no later than 12 months).

95. The copiers and fax devices will operate in special designated rooms, where only personnel authorized to use them shall have access.

96. Based on these regulations, on the regulations and norms of each institution, the security structure/officer shall draft the Security Plan of the objective, approved by the head of the institution and endorsed by the competent institutions. The following elements shall be included in the Security Plan:

a) Delimitation and marking of the security areas;
b) Access control system;
c) Warning and alarm system;
d) Guard and security system;
e) Evacuation of documents in case of emergency ;
f) Actions to be carried out in case of emergency (evacuation/destruction of documents);
g) How to report, investigate and record breaches of security measures;
h) Personnel training and briefing;
i) Responsibilities regarding checks of the security system of the objective;
j) Ways of conducting inspections regarding the security measures of the objective.

F. PERSONNEL SECURITY

97. *Personnel security* means all security procedures applied to individuals who are to be granted access to NATO classified information.

98. Personnel security measures are meant to:

a) prevent unauthorized access to NATO classified information;
b) ensure that NATO classified information is disseminated based on the personnel security clearance certificate and the need-to-know principle;
c) allow the identification of those individuals who, by their actions, might endanger the security of NATO classified information and ban their access to such information.

99. Personnel security is ensured by the following elements: selection, vetting, authorization of access to NATO classified information, revalidation, withdrawal of the security clearance, control and personnel training.

100. The vetting procedure is conducted on individuals who, due to their position or job, need or are going to be granted access to NATO classified information, have to participate in NATO activities or work for a NATO classified contract.

101. Access to NATO classified information, granted by the personnel security clearance certificate issued subsequently to the vetting procedure, is restricted by the need-to-know principle.

102. The vetting process aims at reducing the security risks, the embezzlement or the unauthorized disclosure of NATO classified information and material.

103. The vetting procedure for access to NATO classified information shall be based on the national laws and NATO standards, according to the competences described below:

A. ROMANIAN INTELLIGENCE SERVICE for:

- Its own staff;
- Personnel of public institutions and authorities;
- Personnel of economic units with integral or partial state capital and legal public persons, others than those under the competences mentioned at paragraph B, C and D.

B.MINISTRY OF NATIONAL DEFENSE - GENERAL DIRECTORATE FOR DEFENSE INTELLIGENCE for:

- Its own military and civilian personnel;
- Civilian personnel of enterprises and corporations, scientific, research and development units established by or in cooperation with the Ministry of Defence, or other entities involved in contracts for the supply of military technique, equipment and facilities under NATO contracts, cooperation and assistance programs.

C. FOREIGN INTELLIGENCE SERVICE for:

- Its own military and civilian personnel;
- Romanian staff from embassies, consulates, cultural centers, international organizations, who work abroad and need access to NATO classified information;
- Romanian citizens working abroad on business contracts, scholarships or research programs, employed in state owned or

private companies, involving cooperation with NATO or a NATO structure.

D. MINISTRY OF INTERIOR, GUARD AND PROTECTION SERVICE, and SPECIAL TELECOMMUNICATIONS SERVICE, responsible for their own personnel**.**

104. Whenever necessary, the competent structures responsible for conducting the vetting procedure cooperate, in fulfilling their tasks, on the basis of bilateral protocols.

105. The main criteria of assessing the suitability of an individual in order to be issued a security authorization base on which the security clearance certificate is granted envisage circumstances and character features that might generate security risks. Even if these criteria refer to the individual to be vetted, the behavior, character, conceptions and life circumstances of his/her spouse could also be relevant and should be considered.

106. The factors to be taken into account for the individual and his/her spouse or cohabitant are whether:

(a) has committed or attempted to commit, conspired with or aided and abetted another to commit (or attempt to commit) any act of espionage, terrorism, treason or sedition;

(b) has attempted, sustained, participated in, cooperated and supported espionage or terrorism, or has supported individuals suspected of having committed such crimes, or who are representatives of organizations or foreign nations which may threaten the security of NATO and NATO member or partner states, or are associates of representatives of such organizations;

(c) is or was a member of any organization that supports or attempts to overthrow the government or change the form of government of the NATO member/partner country by violent, subversive or other unlawful means;

(d) is or was a supporter of any organization described in sub-paragraph (c) above, or who is or has recently been closely associated with members of such organizations in such a way as to raise reasonable doubts about the individual's reliability.

107. The additional factors to be taken into account for the individual are whether:

(a) has deliberately withheld, misrepresented or falsified information of security significance, or has deliberately lied in completing the personnel security form or during the course of the security interview;

(b) has been convicted of criminal offences, or offences indicating habitual criminal tendencies; has serious financial difficulties or there is a

striking deference between his/her income and the living standard; has a history of alcohol abuse or drug dependence; has or had promiscuous behavior, sexual misconduct which may give rise to the risk of vulnerability to blackmail or pressure; has demonstrated by act or through speech unreliability, dishonesty, untrustworthiness or indiscretion; has infringed the security regulations;

(c) is suffering or has suffered from any illness or mental condition which may cause significant defects in his/her judgment or may make the individual, unintentionally, a security risk. In all such cases, with the individual's consent, competent medical advice should be sought;

(d) may be liable to pressure through relatives or close associates who could be vulnerable to foreign intelligence services whose interests are inimical to the security interests of NATO and/or member and partner countries.

108. Access to NATO RESTRICTED is granted at the level of each employer institution, based on the authorization given by the security structure/officer, with the approval of the head of the organization.

109. The security clearance certificate is not required for access to NATO RESTRICTED.

110. Level I investigation – to authorize the issuing of NATO CONFIDENTIAL security clearance certificate. The authorization will be based on:

a) check of the correctness of the personal particulars mentioned in the basic vetting form;
b) minimum references from previous employment and groups (three persons at least).

In case certain aspects need further clarification, or at the request of the vetted subject, the investigator may have a meeting with the individual.

111. Level II investigation - to authorize the issuing of NATO SECRET security clearance certificate. This investigation will be based upon:

a) check of the correctness of the personal particulars mentioned in the supplementary vetting form
a) minimum references from the previous employment and groups (three persons at least).
b) investigations conducted on family members against the data given in the form;
c) an interview with the individual.

112. Level III investigation – to authorize the issuing of NATO TOP SECRET security clearance certificate. The authorization to the NATO TOP SECRET will be based on:

a) check of the data provided in the basic, supplementary and financial forms;
b) investigations on the individuals' background at his/her present and former residence, at his/her present and former employments and education since the age of 18. The investigations will not be limited to the persons indicated by the individual;
c) checks on his relation groups to identify possible security risks that may arise;
d) security interview with the individual;
e) psychological test restricted to the field that has to be clarified, to determine the existence of mental disorders, in case the investigations arouse suspicions related to certain psychic deficiencies.

113. If during the investigations, for any level, data revealing security risks result, an additional background inquiry will be conducted, using the specific means of the institutions with tasks in the field of the national security.

114. Depending on the level, the background investigation shall cover the following:

(a) National Records – A check will be made with the national security records and central criminal records, in the central and police records as well as with the database of the Trade Registry.

(b) Birth records and Check of Identity – The individual's date and place of birth will be verified and his/her identity will be checked.

(c) Citizenship – In all cases the citizenship status and/or nationality, present and past, of the individual shall be established.

(d) Education – Investigations will normally cover attendance since 18 of schools, universities and other educational establishments.

(e) Employment – Investigations will cover present and former employment, reference being made to sources such as employment records, performance or efficiency reports and employers or supervisors.

(f) Interviews – Interviews will be held with persons who are in a position to give a true unbiased assessment of the individual's background, activities and trustworthiness.

(g) Records of Central and Local Police – The records of Central and Local Police in the vicinities where the individual has resided or has been employed for substantial periods of time shall be checked.

(h) Military Service – The service of the individual in the armed forces and types of discharge shall be verified.

(i) Foreign Connections – The vulnerabilities to pressure from foreign sources e.g. due to former residence or past associations shall be ascertained whenever possible.

(j) Financial Records –The credit-worthiness and financial standing of the individual shall be investigated.

(k) Organizations – During the course of the investigation, as set forth above, efforts shall be made to determine if the individual has or has had membership in, or affiliation with any foreign or domestic organization, association, movement, group of foreign people or nationals, which has adopted or showed a policy of supporting or approving acts of force or violence in order to deny other persons' rights, or which seeks to alter the form of government of NATO member and partner nations, by unconstitutional means.

115. The type A Personnel Security Clearance Certificate shall be issued based on a written request, signed by the head of the institution and transmitted to the NSA through the Internal Registry.

116. The application shall be accompanied by the vetting forms, filled in by the applicant and enclosed in a separate sealed envelope.

117. The security structure/officer shall make available to the candidate the vetting forms corresponding to the access level for which the security clearance is requested. He shall assist the applicant in filling in these forms, and shall observe the deadlines for sending the request to the NSA, taking into account the date when the candidate is presumed to have access to NATO classified information, as follows:

a) access to NATO TOP SECRET – 3 months in advance;
b) access to NATO SECRET – 2 months in advance;
c) access to NATO CONFIDENTIAL – 1 month in advance.

118. Within 7 days from the date when the request was received, NSA shall send to the relevant institution the request for initiating the vetting procedure on the candidate, to which the sealed envelope containing the vetting forms shall be attached.

119. After receiving the forms, the relevant institution shall conduct the vetting and shall send the results, in writing, to the NSA, observing the above-mentioned deadlines. The results will indicate whether there is a security risk related to the vetted individual.

120. For its own personnel from Romanian Intelligence Service, Ministry of Defence, Foreign Intelligence Service, Ministry of Interior, Special Telecommunications Service and Guard and Protection Service, these institutions shall notify to the NSA the initiation of the vetting procedure, and the type A personnel security clearance certificate shall be issued following a written request to the NSA signed by the head of the institution. The written request will indicate that the vetting was conducted and will

contain the conclusions on existence/non-existence of security risks or other security relevant aspects.

121. Type B certificates of security clearance shall be issued only to those persons holding a type A personnel security clearance certificate.

122. Type B certificate of security clearance shall be issued by the relevant security structure/officer, with the approval of the head of the organization where the individual works. If a security structure/officer is not established, the institution shall request the NSA to issue the certificate. In this case, the request shall be sent to the NSA, at least 2 weeks before the beginning of the activity for which the certificate is necessary.

123. The certificate of security clearance is issued based on the analysis of the vetting results sent by the competent institution. In case there are indications of security risks, NSA will decide if these could impede the issuing of the certificate. When there are indications of certain aspects that are not security risks, but are relevant from the security viewpoint, security interests will prevail in issuing the certificate.

124. NSA has 7 days at its disposal to issue the certificate or to communicate the refuse of issuing it to the requesting institution.

125. A copy of the letter informing about NSA's decision of granting/not granting the personnel security clearance certificate shall be sent to the institution that conducted the vetting.

126. Type A personnel security clearance certificate is issued in two original copies. One is kept at the Central Registry and the other at the organization where the candidate works.

127. The validity of the type A personnel security clearance certificate is of 3 years.

128. A copy of the type B certificate of security clearance is kept by the security structure/officer of the institution where the candidate works.

129. A new vetting shall be conducted if it is necessary that a candidate be issued a new security clearance certificate, if there are indications of security risks, or at NATO request. A new PSC certificate can be issued at the request of the institution, in the following cases:

a) if, in fulfilling his duties, the individual needs access to a higher level of NATO classified information;
b) if the validity of the previous PSC certificate has expired;

c) if there are changes in the identification data of the individual, data that appear on the PSC certificate, the old certificate is withdrawn and a new one shall be issued.

130. A new vetting will be conducted, without issuing a new certificate of security clearance, in the following cases:

a) if there are changes in the data provided by the individual in the vetting forms, except for those under subparagraph 129 letter c);
b) if, during the validity period of the PSC certificate there are indications of security risks;
c) if NATO structures or NSAs from NATO member or partner countries request that a new vetting be conducted.

131. The National Security Authority is the only institution empowered to withdraw the security clearance certificate. NSA shall inform the institution on the decision to withdraw a security clearance certificate.

132. Type A and B certificates of security clearance shall be withdrawn in the following cases:

a. at the initiative of NSA;
b. at the request of the institutions that applied initially for the issuance of the certificates, including the case of expired validity;
c. when the individual leaves the institution or changes his working place, if the new job does not involve working with NATO classified information;
d. changes of the level of access.

133. In case the security clearance certificate is withdrawn, the individual shall be forbidden access to NATO classified information.

134. After withdrawal, type A and B certificates of security clearance will be destroyed based on a certificate of destruction. The institution that conducted the vetting shall be informed of this.

G. DOCUMENT SECURITY

135. The North-Atlantic Council (hereinafter NAC) is the supreme authority for the release of official NATO classified information to member and partner states. This authority functions on the originator's consent principle.

136. All transfers of documents from NATO to partner countries shall be done through the NATO Registry to the Central Registry of the partner state. The released documents refer to actions, activities, etc approved by the NAC.

137. NATO bodies shall keep, as originator, the accountability of all NATO classified information released to partner states and shall send the identification data of these documents (number, title and date of release) to the NATO Central Registry in Brussels. At request, the national authorities can obtain details from the NATO Central Registry in Brussels.

138. NATO UNCLASSIFIED information, although not requiring special protection, may be released to non-NATO nations, organizations and individuals when such release is not against the interest of the North-Atlantic Treaty Organization.

139. NATO classified information needs special protection and may be circulated according to the need-to-know principle and without reference to the originator, but only specifying “NATO”. The initial information remains the property of the originator, which is the only authority to decide on its classification level and release, and may not be transmitted to any non-NATO nations or to any other international organization, except with the originator’s approval.

140. NATO classified documents are managed according to NATO procedures on the protection of NATO classified information, within the National Registry System, by cleared individuals, holding personnel security clearance certificates for the appropriate classification level.

141. NATO classified documents, as well as national classified documents released to NATO by Romania, shall be managed separately from the national classified documents.

142. NATO UNCLASSIFIED information is not subject to the security procedures for NATO classified information. NATO UNCLASSIFIED information shall be managed in accordance with the existing domestic norms for national information with equivalent level of classification, so that the interests of the North Atlantic Alliance should not be harmed.

143. Classification of NATO information is necessary to indicate the sensitivity of information, and, consequently, the level that must be assigned to it in order to establish the complexity of the measures and procedures required to protect this information against unauthorized disclosure.

144. The classification levels require that, on the one hand, security measures for the protection of classified information, in accordance with NATO standards, be ensured, and, on the other hand, control of access to such information.

145. The responsibility for assigning a security classification to information and material rests with the originator of the information/material and shall be done accordingly to the importance and contents of the information. Both over-classification and under-classification of the documents are dangerous.

146. The hierarchical chief of the document's originator shall check whether the classification levels were correctly assigned and shall take the necessary measures for a correct classification in case of inappropriate classifications.

147. The classification level of documents received from other institutional structures shall be changed only with the approval of the document's originator.

148. Letters accompanying the documents shall be classified according to their content, regardless the classification level of the document.

149. Excerpts from documents containing NATO classified information shall be classified according to the content of the information in the document, the classification level being at least equal to that of the document where the excerpt was extracted from.

150. Depending on the importance and sensitivity of the information, NATO classification levels and their equivalences in the national legislation are:

ROMANIA	NATO
SERVICE SECRET	RESTRICTED
SECRET	CONFIDENTIAL
STRICT SECRET	SECRET
STRICT SECRET DE IMPORTANCE DEOSEBITA	TOP SECRET

151. Taking into account the risks generated by unauthorized disclosure of NATO classified information, the classification levels shall be assigned according to their importance, meaning:

- NATO/RESTRICTED - SECRET DE SERVICIU: classification level applied to information and material the unauthorized disclosure of which would be disadvantageous to NATO and national interests.

- NATO/CONFIDENTIAL – SECRET: classification level applied to information and material the unauthorized disclosure of which would be damaging to NATO and national interests.

- NATO/SECRET – STRICT SECRET: classification level applied to information and material the unauthorized disclosure of which would result in grave damage to NATO and national interests.

NATO/TOP SECRET – STRICT SECRET DE IMPORTANTA DEOSEBITA: security classification applied to information and material the unauthorized disclosure of which would result in exceptionally grave damage to NATO and national interests.

152. According to the security agreements signed so far, NATO shall release to partner countries classified information marked NATO up to SECRET level included.

153. NATO classified information may be downgraded or declassified only by, or with the originator's consent, and only after the other member nations and organizations have been consulted.

154. The downgrading shall be done periodically following a special review which will establish whether the initial classification level of the document is still consistent with its informational value at the time of the review.

155. The change of the classification level of a document shall be immediately notified to all the addressees of that document.

156. *Declassification* means annulment of the classification level of NATO classified information i.e. its removal from under the incidence of all regulations for the protection of NATO classified information.

157. NATO CONFIDENTIAL and NATO SECRET information shall be systematically reviewed for declassification (only after a period of at least 30 years).

158. The marking NATO applied to a document signifies that the document is the property of NATO and that the information contained remains the property of the originator. The marking NATO shall be applied to all copies prepared for circulation within the North-Atlantic Treaty Organization, including NATO UNCLASSIFIED documents.

159. All documents containing NATO classified information, including files, volumes, or brochures, or reproductions of these, shall be marked in writing or printing at the top and bottom of the first page (cover), on the title page, the first page, the last page and on the outside of the back cover. The classification level assigned by the originator shall be marked at the top and bottom of each page of the document.

160. All documents released by NATO shall maintain the classification level assigned by the North Atlantic Alliance all through their existence. The first page will bear the name of the NATO structure that authorized the release, the date when the release was decided and other related elements.

161. In case a classified document is released by NATO following the carrying out of a common activity approved by the NAC, the classification shall be preceded by the mark NATO and the name of an activity, country or organization.

Example: NATO/EAPC/PfP CONFIDENTIAL or
NATO/ROMANIA CONFIDENTIAL or
NATO/OSCE CONFIDENTIAL

162. In case the originator of the document deems necessary to restrict the release of the classified information, this shall be marked under the demarcation line, by indicating the name/names of the country(ies) receiving the document

Example: NATO/PfP CONFIDENTIAL
ROMANIA/BULGARIA only

or

NATO/PfP CONFIDENTIAL
EXERCISE COPPERPLATE only

163. The documents released by Romania to NATO will bear the mark ROMANIA, followed by the classification level (equaled to the NATO classification level) and the structure/activity within NATO that the document is released to.

Ex.

ROMANIA-CONFIDENTIAL	ROMANIA-SECRET
NATO only	PfP only

164. The minimum requirements for the management of NATO classified information shall apply depending on the classification level.

165. NATO/RESTRICTED information shall be handled and stored in places not accessible to unauthorized individuals.

166. The documents will be transmitted by channels authorized by the NSA, in accordance with the existing procedures. The cryptographic systems approved by a NATO nation or by NAMILCOM shall be used for

encrypting NATO RESTRICTED information transmitted by electronic means.
In emergency cases, when speed is essential and encryption means are not available, NATO RESTRICTED information may be transmitted in clear text, by public communication systems.

167. Copying and translation of NATO RESTRICTED documents shall be made within the CNRS, with the strict observance of the need-to-know principle.

168. NATO CONFIDENTIAL information shall be handled and stored in areas with strictly controlled access. Access shall be allowed only to those individuals holding a security clearance certificate and approval for such access.

169. Documents shall be transmitted by special courier or diplomatic pouch.

170. Cryptographic systems approved by a NATO member nation or by NAMILCOM shall be used for encrypting NATO CONFIDENTIAL information transmitted by electronic means.

171. Copying and translation of NATO CONFIDENTIAL documents shall be made by authorized persons, observing the need-to-know principle.

172. NATO SECRET information will be handled and stored in areas with strictly controlled access. Access will be allowed only to those individuals holding an appropriate security clearance certificate and who need access to such information in fulfilling their duties.

173. Documents will be transmitted by special courier or diplomatic pouch. Only cryptographic systems approved by NAMILCOM shall be used for encrypting such information.

174. Copying and translation of NATO SECRET documents shall be made by the individual holding them, in accordance with the need-to-know principle, only with the written approval of the originator. The copies of NATO SECRET documents shall bear the copy number; the number assigned to copies/translations of such documents shall be recorded in the respective component of the CNRS.

175. Management of NATO classified documents entails:

- Reception of documents - is the activity of unsealing and unpacking the documents received.

- Check means:
    a. check the seals, envelopes and wrappings;
    b. check the documents accompanying the main document (letters, dockets etc);
    c. check the document integrity;
    d. check the correspondence between the number of pages written on the docket and of the document; the same is valid for the annexes .
    e. check the compulsory markings on the document;

Record – means recording the document in the registry of the respective CNRS and marking the document with the relevant number assigned in the registry.

Consultation – NATO classified documents shall be consulted by authorized individuals only, against signature, with the observance of the need-to-know principle.

Dissemination – activity of distributing the documents, according to the need-to-know principle.

Transmission – activity of circulating NATO classified documents within the National Registry System and between the NRS and NATO.

Transport – refers to the way NATO classified documents are circulated between the sender and the recipient.

Multiplication – activity of copying NATO classified documents. The number of copies shall be recorded in a special registry.

Destruction – activity of shredding, burning, melting those documents which are no longer necessary to be kept; it is done differently, depending on the document classification level and after the inventory of the documents which will still be kept, has been made.

Inventory – annual activity of checking the existence of documents and re-recording those which are still needed.

Archiving – activity of storing, in specially designed places, documents that were not destroyed, but still considered necessary, and which do not need to be kept together with the documents currently in use.

H. INDUSTRIAL SECURITY

176. In order to fulfill its duties in the field of protection of NATO classified information, the National Security Authority appoints as Designated Security Authorities the institutions with responsibilities in the civil and military industrial field. To this end, these authorities have the following duties:

a) to implement the national security policy in the industrial field, to guide and provide the necessary assistance in enforcing this policy;

b) to impose the observance of the industrial security norms at national level (they have the right to supervise and approve the standards on the protection of NATO classified information);

c) to monitor the compliance of the components of a NATO classified contract or sub-contract in accordance with NATO standards. Before releasing NATO classified information to an economic unit during the carrying out a NATO classified contract, the following requirements shall be accomplished by the unit:

- to ensure protection measures according to these regulations;
- to hold facility security clearance;
- the individuals involved in a NATO classified contract must have personnel security clearances for the level of classification of NATO information they have access to;
- the access to classified information disseminated within the contract is allowed only to the persons working on that contract, with the observance of the need-to-know principle.

d) to issue, at the request of a NSA from a NATO member state, facility security clearance to an economic unit involved in negotiating or carrying out of a NATO classified contract or sub-contract;

e) to issue, at the request of a NSA from a NATO member state, personnel security certificate to the persons involved in negotiating or carrying out a NATO classified contract or sub-contract;

f) to designate, in the industrial entities involved in carrying out a NATO classified contract or sub-contract, a security structure/officer with specific duties according to the type of contract;

177. In order to issue a facility security clearance for the economic units involved in carrying out a NATO classified contract, one will check if the security requirements on the protection of NATO classified information are met, in accordance with the classification level of the information disseminated within the contract or sub-contract.

178. For the individuals involved in carrying out NATO classified contracts, personnel security clearance certificates will be issued, consistent with these regulations.

I. INFOSEC

179. The security policy and requirements of this section shall apply to all Automatic Data Processing (ADP) Systems, Data Transmission Networks (DTN), as well as Communication and Information Systems (CIS) storing, processing or transmitting NATO classified information. These systems shall require security measures to ensure the protection of the information and especially to control the access to the information, based on the “need-to-know” principle and on the security level assigned.

180. Protection ADP and/or DTN (CIS) of weapons and detection systems shall be defined in the general context of the systems to which they belong, and shall be done by enforcing the provisions of this section.

181. Protection of NATO classified information, which is stored, processed or transmitted in ADP and/or DTN (CIS) systems, is ensured by the National Security Authority, through the following agencies: Security Accreditation Agency (SAA), Communication and Information Security Agency (CISA), Cryptographic Material Distribution Agency (CMDA).

182. The Security Accreditation Agency (SAA) is responsible, at national level, for the security accreditation and implementation of NATO security policy in compliance with the CIS accreditation.

183. The Security Accreditation Agency (SAA) is responsible for granting approval to an ADP and/or DTN (CIS) system to store, process or transmit NATO classified information, up to a defined classification level (including, where appropriate, special categories) in its operational environment. The Security Accreditation Agency is responsible for the evaluation and certification of the ADP and/or DTN (CIS) systems or some of their components.

184. The Security Accreditation Agency (SAA) is a national accreditation structure, subordinated to the National Security Authority (NSA), with delegated/ nominated representatives from the departments involved, depending on the ADP and/or DTN (CIS) system to be accredited. The SAA shall be responsible for the periodical re-accreditation process of the ADP and/or DTN (CIS).

185. The SAA exercises its responsibility in the security field on behalf of the NSA, it is responsible for the security in all but some special cases, and is authorized to enforce security standards.

186. The SAA establishes the security accreditation strategy, as part of the NSA overall security policy, and clearly states the conditions under which it is called upon to accredit an ADP and/or DTN (CIS) system.

187. The CISA is the structure, acting at national level, subordinated to the NSA, having representatives delegated/ nominated by the NSA within the involved departments. The CISA exercises its authority at local level, through the Local Operational Authority of the CIS (CISLOA). The CISA bears the responsibility for conceiving and implementing the ways and means of protection for the NATO classified information, which is stored, processed or transmitted through the CIS, having essentially the following responsibilities:

a) Coordinating all the protection activities for the stored, processed and transmitted NATO classified information;
b) Conceiving and promoting specific standards and regulations;
c) Analyzing the causes of security incidents and database administration concerning the vulnerabilities of the information and communication systems required for the risk management of CIS security systems ;
d) Submitting the security incidents to SAA ;
e) Integrating measures regarding physical, personnel, documents, administrative, cryptological, COMPUSEC, COMSEC, TEMPEST protection;
f) Fulfilling periodical inspections on ADP systems and/or networks (CIS) for their re-accreditation by SAA;
g) Submitting CIS-specific security systems to certification and authorization;
h) Cooperating with the SAA, the CMDA, as well as with other responsible security bodies.

188. The CMDA is a national structure subordinated to the NSA, and responsible for:

-Management of NATO-specific cryptographic material and equipment;
- Distribution of NATO-specific cryptographic material and equipment;
- Periodical reports to CISA of the encountered security incidents;
- Cooperation with the SAA, the CISA and other involved security bodies.

189. A threat can be defined as an accidental or deliberate potential compromise of ADP or DTN (CIS) system or network security by loss of confidentiality, loss of integrity or loss of availability of information in electronic format.

Vulnerability can be defined as a weakness or lack of control that would allow or facilitate a threat actuation against a specific asset or target and may be technical, procedural or operational in nature.

190. The security measures in this section applies to the CIS systems storing, processing or transmitting information classified NATO CONFIDENTIAL and above.

191. A balanced set of security measures (physical, personnel, administrative, TEMPEST-type measures regarding computer and communication) shall be identified and implemented to create o secure environment in which an ADP and/or DTN (CIS) system or network (CIS) operates.

192. The CIS security measures shall grant control of the access, in order to prevent or detect the unauthorized disclosure of information. The process of certification and accreditation shall determine the adequacy of CIS security measures.

193. The Specific Security Requirement Statement (SSRS) form a binding agreement between the SAA and the CISLOA as a complete set of security principles to be observed and of detailed security requirements to be implemented, underlying the process of certification and accreditation of ADP systems and/or network (CIS).

194. SSRS is developed for all ADP and/or DTN (CIS) systems which store, process or transmit NATO classified information. These requirements are set up by CISLOA and approved by SAA.

195. The SSRS shall be formulated at the earliest stage of ADP and/or DTN (CIS) project and shall be developed during the whole life cycle of the system.

196. The SSRS is based on NATO security policy and risk assessment put forward by the NSA, taking into consideration the essential parameters covering the operational environment, the lowest level of personnel clearance, the classification level of information and the operation mode of the system to be accredited.

197. All ADP systems and/or DTN (CIS) network storing, processing or transmitting NATO classified information shall be certified and accredited to operate during certain time frames and in different modes of operation, as follows:

a) dedicated;
b) system-high; and
c) multi-level.

198. “***DEDICATED”***

In this mode of operation ALL individuals with access right to the ADP systems and/or DTN (CIS) are cleared to the highest classification level for the information stored, processed or transmitted within the ADP system and/or DTN (CIS). The "need-to-know" principle for these persons applies to all information stored, processed or transmitted within the ADP system and/or DTN (CIS).

(1) in this mode of operation, the "need-to-know" principle does not imply a mandatory requirement for the separation of information within the ADP system and/or network (CIS), as a means of CIS security.

(2) other security features (for example: physical, procedural and personnel) must conform to the requirements imposed for the highest classification level and all category designations of the special destination information stored, processed or transmitted within the ADP system and/or network (CIS).

199. “***SYSTEM HIGH”***

In this mode of operation all individuals with access right to the ADP system and/or DTN (CIS) are cleared to the highest classification level for information stored, processed or transmitted within ADP system and/or DTN (CIS), but the individual access to the information is differentiated, according to the "need-to-know" principle.

(1) The fact that in this operation mode the access to information is differentiated, according to the "need-to-know" principle, indicates that there must be - as a compensation- some security facilities which shall provide a selective access to the information within ADP system and/or network (CIS);

(2) The other security features (for example: physical, procedural or personnel) must conform to the protection requirements for the highest classification level and for all category designations of special destination information stored, processed or transmitted within the ADP system and/or network (CIS);

(3) All information stored, processed or transmitted within ADP system and/or DTN (CIS) under this mode of operation shall be protected as information with a special designation, having the highest classification level.

200. “***MULTI-LEVEL”***

In this mode of operation, not all personnel entitled to access the ADP system and/or DTN (CIS) have personnel security clearance for access to information of the highest level of classification, which is stored, processed or transmitted through the ADP system and/or DTN (CIS). In a

similar manner, not all individuals having access to the ADP system and/or DTN (CIS), may also access all information stored, processed, transmitted within the ADP system and/or DTN (CIS), the access to this information is selectively made, according to “need to know” principle.

(1) This protected operation mode allows storing, processing and transmitting of information at different levels of classification and having different destinations;

(2) Since not every individual is authorized for the highest level of classified information, and also since the access to information is made selectively, according to “need to know” principle, there have to be compensatory security facilities meant to ensure a selective access mode to information within ADP system and/or network (CIS).

201. CIS LOCAL OPERATIONAL AUTHORITY (CISLOA) is the person or department delegated with responsibility by the CISA over the ADP system and/or DTN (CIS), in order to implement the necessary means and ways for information protection, as well as for the secure operation of the ADP systems and/or network (CIS). The CISLOA responsibility extends throughout the entire life cycle of the ADP system and/or DTN (CIS), starting with design, going on with the development of the specifications, installation testing, and accreditation, periodical testing for re-accreditation, operational exploitation and modification, up to the final disposal. In some special circumstances, the CISLOA role may be transferred to different components of the organization, during the life cycle. It is important for this role to be identified and exercised from the beginning, without interruption throughout the life cycle.

202. The CISLOA coordinates the cooperation between the body having the authority over the CIS of an organization and the security accreditation structure, when the organization:

a. plans to develop or acquire an ADP system and/or DTN (CIS);
b. proposes changes to an existing system configuration;
c. proposes to interconnect an ADP system and/or DTN (CIS) with another ADP system and/or DTN (CIS);
d. proposes changes to the security mode of operation of an existing ADP system and/or network (CIS);
e. proposes changes to existing programs, or to use new software packages, which may have an impact on ADP system and/or network (CIS) security;
f. proposes to modify the security classification level for an ADP system and/or network (CIS), which has been already accredited;
g. plans, proposes or intends to undertake any other activity that may affect the security of an already accredited ADP system and/or network (CIS) (for instance, the substantial increasing in the number of users).

203. The CISLOA directed by the Security Accreditation Authority and in cooperation with the structure exercising authority over CIS, decides on the security standards and procedures to be observed by the equipment supplier during the development, installation and testing of the ADP system and/or network (CIS). The CISLOA is also responsible for the justification, selection, implementation and control of those technical components ensuring the security, and which are parts of the overall ADP system and/or network (CIS).

204. From the very conception, CISLOA assigns the necessary responsibilities to be fulfilled throughout the entire life cycle of the ADP system and/or network (CIS) to security and management structures of the ADP system and/or network (CIS).

205. The CISLOA or the delegated competent structure appoints the CIS Site Security Officer responsible for ensuring the implementation and maintenance of the physical security measures applied to the respective site.

206. A CIS site may be a particular location, or a group of locations where an ADP system and/or a DTN operates. The responsibilities for each location of a remote terminal/workstation must be clearly identified. The responsibilities of a CIS Site Security Officer may be carried on by the organization security officer, as part of his professional duties.

207. The ADP system Security Officer is appointed by the CISLOA, to be responsible for the supervision of the development, implementation and management of the security measures within the ADP system, including the preparation of Security Operating Procedures (SecOPs;). Following the recommendation of the Security Accreditation Authority, additional persons will be nominated by CISLOA (for instance, for specific directorates or divisions of an organization) who carry out these security duties according to the conditions set out by the ADP System Security Officer within the framework of the Security Operating Procedures.

208. For a single large ADP or for several interconnected ADP Systems, a Network Security Officer responsible for managing the network communication security within network is appointed by CISLOA.

209. All ADP system and/or network (CIS) users are responsible for the security of their ADP system and/or network (CIS) (essentially, according to the conferred rights), and are under the guidance of Security Officers. Briefing and awareness of all users about their security duties grant an increased efficiency of the security system.

210. The CIS security education and training are to be adequately ensured at various levels, and for various personnel classes within an organization, such as: senior management level, Security Authority staff, Security Officers, users, etc. and are in conformity with the general training plan of National Security Authority.

211. Users of the ADP system and/or DTN (CIS) are cleared and allowed access to classified information according to the “need to know” principle and depending on the classification level of the information stored, processed or transmitted within a particular ADP system and/or DTN (CIS).

212. Due to information vulnerability to: unauthorized access, denied access, disclosure, corruption, modification or deletion, special measures are foreseen in order to train and supervise the staff, also including the system design personnel having access to the ADP system and/or network (CIS).

213. The ADP system and/or network (CIS) must be designed in such a way to allow assignment of tasks and responsibilities to personnel so as to avoid that one person has complete knowledge or access to all the security keys (passwords, personal identification devices, etc.) and to all programs.

214. The operating procedures for the personnel within the ADP system and/or network (CIS) must ensure a clear segregation between programming and system/network operation. Save for special circumstances, members of the personnel are prohibited from both programming and operating the systems or networks, and appropriate procedures must be established in order to prevent such activities.

215. For any alteration applied to an ADP system and/or DTN (CIS), the cooperation of at least two persons is mandatory. The security procedures must clearly state those situations where the two men rule is implemented.

216. In order to ensure that the security measures are properly implemented, the ADP system and/or network (CIS) staff and the personnel responsible for the ADP system and/or network (CIS) security are trained and briefed so as to be mutually acquainted with each other’s responsibilities.

217. The ADP system / DTN locations and remote terminal areas where NATO classified information is presented, stored, processed or transmitted or the places where the access to such information is possible, are stated security areas, defined in Physical Security section.

218. The following general security measures are applicable to ADP and remote terminal/workstation areas, where NATO classified information is processed or accessed:

a) Entry of both personnel and materials to, and their departure from these areas are controlled by well defined means;
b) ADP and remote terminal/workstation areas and locations where the ADP system and/or network (CIS) security may be modified shall never be occupied by a single authorized employee;
c) Individuals requiring temporary or intermittent access to these areas shall be authorized as visitors by the CIS Site Security Officer, according to his attributions. Visitors are permanently accompanied to ensure that they are denied access to NATO classified information or to the equipment in use.

219. Depending on the security risk, and on the classification level of the information being stored, processed and transmitted, the two men rule may be enforced to other areas too. Such areas are established during the project inception stage and are specified within the Specific Security Requirement Statement (SSRS).

220. When an ADP system is operated in a stand-alone mode, permanently disconnected from another ADP system and/or network (CIS), then taking into account specific environmental conditions, other procedural or technical security measures, and the part played by that ADP system within the overall operation, the Security Accreditation Authority (SAA) may waive the requirement of paragraph 218(b). In such cases, the Security Accreditation Authority shall establish adequate rules adapted to the ADP system structure, according to the classification level of information being processed and shall identify special features.

221. All information and material controlling access to an ADP system and/or network (CIS) shall be controlled and protected under arrangements appropriate for the highest level of classification and the category designation of the information to which the ADP system and/or network (CIS) allow access.

222. When no longer in use, the information and control material specified under paragraph 221, shall be destroyed.

223. The originator of information shall identify and classify, or indicate as unclassified, all information-bearing documents, either on hard-copy output or computer-storage media. Regardless of its form, each document shall be marked with its own classification level. The document media shall have the same level as the highest classification level of the information used for creating the documents referred to. Equally, they may be classified according to the highest classification level of an ADP system and/or DTN

(CIS), operating in DEDICATED MODE, or in SYSTEM HIGH MODE, unless the originator or high authority responsible for release of information has established, after review, a different classification.

224. The information owners must analyze the problems of information aggregation and the ensuing consequences on the classification level, in order to determine whether a higher level of classification is appropriate for the aggregated information.

225. The information output layout using brevity code, transmission code or any binary representation does not provide any security protection and hence, should not influence the classification level assigned to the information referred to.

226. The documents containing NATO classified information shall be controlled according to the current security regulations, prior to their release from the ADP system and/or network (CIS) areas, or from remote terminal areas.

227. When information is transferred from an ADP system and/or network (CIS) to another ADP system and/or network (CIS), it shall be protected both during transfer and within the receiving ADP system and/or network (CIS), according to the original classification and category of the information.

228. All computer storage media are preserved according to the highest classification level of the stored information or media label, being at all times appropriately protected.

229. Re-usable information storage media, used for recording NATO classified information, maintain the highest classification level for which they have ever been used, until the respective information is downgraded to a lower classification level or marked as unclassified. In this case, the above mentioned media must be reclassified accordingly, or must be destroyed in compliance with the SecOPs provisions.

230. Automatic or manual logs are being kept as a record of access to information classified NATO SECRET and above. These records shall be kept for a certain period of time, decided by mutual agreement between SAA and CISLOA. With respect to the records regarding access to the NATO information classified COSMIC TOP SECRET, or Special Category information, the minimum retention period is 10 years; for information classified NATO SECRET, the minimum retention period is 3 years.

231. The storage media containing NATO classified information used within an ADP area can be handled as one classified item, and need not be

registered within the Central Registry or Sub-Registries, provided that the material is identified, marked with its classification level and controlled within the ADP area, until it is destroyed, reduced to a record copy or placed on a permanent file. The records and control of classified materials are kept within the ADP area, until they are submitted to a document accountability control or destroyed.

232. When material is generated within a CIS, and it is afterwards transmitted to a remote terminal/workstation, appropriate security measures are taken, in agreement with the Security Accreditation Authority (SAA). The procedures shall also contain specific instructions with respect to the accountability of information.

233. All removable computer storage media classified NATO CONFIDENTIAL and above, are appropriately identified and controlled (for NATO UNCLASSIFIED and NATO RESTRICTED, local security regulations, approved by the National Security Authority, shall apply). The identification and control shall include at least the following requirements:

a) for NATO CONFIDENTIAL and above:
   - a means of identification (serial number and classification level marking), separately for each storage media (noting that the marking must indicate the highest classification level ever stored on it, unless downgraded according to the approved procedures);
   - fixed procedures for issuing, receiving and final disposal of the storage media, in order to be destroyed or other purposes;
   - manual or printed records indicating the general content, classification and category designation of the information;
b) for NATO SECRET level and above, detailed information regarding the removable storage media, including the content and classification level, must be kept within an appropriate registry;

234. Spot-checking and overall mustering of removable storage media in order to ensure consistency with the identification and control procedures in place:

a) for NATO CONFIDENTIAL level, removable computer storage media are periodically spot-checked for their physical presence and contents, in order to ensure that those storage media do not contain information with a higher classification level;
b) for NATO SECRET level, all removable storage media are periodically mustered, and spot-checked for their physical presence and contents, in order to ensure that those media do not contain information with a higher classification level;
c) for NATO COSMIC TOP SECRET level and Special Category information, all removable storage media are mustered, on an

annual basis, and are periodically spot-checked for their physical presence and contents, in order to ensure that no Special Category information is inappropriately stored on the respective media.

235. Users must take the responsibility of ensuring that NATO classified information is stored on media with the appropriate classification marking and protection. Procedures shall be established to ensure that, for all classification levels of NATO information, the storage of the information on computer storage media is being carried out according to security regulations.

236. NATO classified information recorded on re-usable storage media is erased only in accordance with the SecOPs.

237. When a storage medium comes to the end of its useful life, it must be de-classified and can be then released and handled as unclassified. If the medium cannot be de-classified, it must be destroyed by an approved procedure. Storage media containing NATO COSMIC TOP SECRET or Special Category information can be destroyed, but cannot be de-classified and reused.

238. NATO classified information stored on non-reusable media (punched cards or tapes, printout material etc.), shall be destroyed according to the Document Security provisions, stipulated in chapter G.

239. All means used for the electromagnetic transmission of NATO classified information follow the current NATO communications security instructions promoted by the National Security Authority.

240. An ADP system (CIS) must be provided with the necessary means for completely denying access to NATO classified information from all remote terminals/workstations, when required, by physical disconnection or by special software features approved by SAA.

241. Initial installation of CIS and any major change within, shall be carried out by authorized personnel only. They are under the constant supervision of technically qualified personnel who are cleared for access to NATO classified information of the highest level, which the respective CIS is expected to store, process or transmit.

242. All equipment is installed according to the current NATO specific regulations promoted by the NSA. National directives of technical equivalence may also be used.

243. CIS systems storing, processing and transmitting information classified NATO CONFIDENTIAL and above, shall be appropriately protected against security vulnerabilities caused by compromising emanations, the study and control of which is referred to as “TEMPEST”.

244. Information processing is carried out according to the Security Operating Procedures (SecOPs).

245. Release of information classified NATO CONFIDENTIAL and above to unmanned facilities is prohibited unless specific regulations approved by the Security Accreditation Authority (SAA) and specified by the SecOPs are applied.

246. Information classified NATO COSMIC TOP SECRET and Special Category information cannot be stored, processed and transmitted within CIS that have potential or authorized users not possessing a security clearance certificate.

247. SecOPs are a description of the security policy implementation to be adopted, of the operating procedures to be followed and of the personnel responsibilities.

248. SecOPs are established by CISA in agreement with CISLOA and the SAA which are also coordinating other security elements involved. SAA shall approve the SecOPs before authorizing the storing, processing or transmitting of information classified NATO CONFIDENTIAL and above.

249. CISLOA shall establish controls ensuring that master copies of all software products (general-purpose operating systems, subsystems and software packages) in use, are protected according to the classification level of the information they have to process. Security protection of software applications shall be established in the first place on the basis of an assessment of their level of security classification and then the classification level of the information to be processed, shall be taken into consideration.

250. The software versions in use have to be verified at regular intervals in order to ensure the integrity and correct functioning. New or modified versions of software shall not be used for the processing of information classified NATO CONFIDENTIAL and above, until software security features have been tested and approved by the ADP System Security Officer. New and/or modified versions of software also depend on the re-accreditation conditions specified by the SSRS, approved by SAA. Software providing new or alterable capabilities and containing no security features cannot be used until verified by CISLOA.

251. The checking for software viruses and malicious software is carried out according to the requirements of SAA.

252. New and/or modified software versions (operating systems, subsystems, software packages and applications software), stored on various media, to be introduced in an institution/structure/organization, shall be verified (mandatory on stand-alone computer systems), in order to identify malicious software or computer viruses, before usage within the ADP system or network (CIS). Additionally, installed software shall be periodically verified; these checks shall be done more frequently, if ADP system and/or network (CIS) is connected to another ADP system and/or network (CIS) or to a public telephone/data transmission network.

253. Maintenance contracts for the ADP systems and/or network (CIS) that store/process/transmit information classified NATO CONFIDENTIAL and above, shall specify the requirements to be met by the maintenance personnel and their specific equipment in order to be introduced in the ADP system and/or network (CIS) area. The maintenance personnel must possess security clearance certificates, since NATO classified information may be accessed while carrying out maintenance operations.

254. The requirements mentioned in paragraph 253shall be clearly stated in SSRS, and the procedures of carrying out the above-mentioned activities shall be clearly stated by SecOPs. Maintenance operations, requiring remote access diagnostic procedures shall be permitted if and only if the respective activities are carried out under stringent security control, and only with the approval of the SAA.

255. Procurement of ADP systems or DTN is limited, as much as possible, to ADP systems or DTN designed and manufactured in NATO member countries. Hardware and/or software developed and /or manufactured in non-NATO member countries may be procured only with the approval of SAA.

256. For CIS storing, processing and/or transmitting information classified NATO SECRET and above, and/or Special Category information, the respective CIS or their baseline security products (such as general-purpose operating system products, security-enforcing limited functionality products and products for network communication), may be procured only if they have been or are going to be evaluated and certified by SAA, in accordance with the NATO criteria (AC/35 – D/1012 revised) or equivalent national criteria.

257. For CIS storing, processing and/or transmitting information classified NATO CONFIDENTIAL, the systems and their baseline components shall observe, as much as possible, the criteria stated in paragraph 256.

258. In deciding whether equipment, particularly specific storage media, should be leased rather than purchased, it should be taken into account that such equipment, once used for storing and processing NATO classified information, cannot be taken out of the protected area, unless previously being de-classified to the approval of SAA, which is not always possible.

259. All ADP systems and/or networks (CIS), prior to be used for storing, processing, or transmitting information classified NATO COFIDENTIAL and above, shall be accredited by SAA, based upon information provided by SSRS, SecOPs and any other relevant documentation. ADP and/or network (CIS) subsystems as well as remote terminals /workstations shall be accredited as part of all CIS to which they are connected to. When an ADP system and/or network (CIS) supports both NATO and national organizations/structures, the NATO and NSA shall mutually agree on the accreditation.

260. In certain instances, prior to CIS accreditation, the multi-level security mode of operation requires previous evaluation and certification accomplished by SAA for hardware, firmware and software security features of the CIS. These activities are based on the compliance with NATO criteria (or national criteria approved by SAA), regarding their capabilities of safeguarding NATO information of different classification level and category designation, and of discriminating between users on the basis of their authorized access to the system.

261. The requirements for evaluation and certification are included in the CIS planning, and are clearly stated in the SSRS, as soon as the security mode of operation has been established.

262. The instances where evaluation and certification must be required, within the multi-level security mode of operation, are as follows:

a) ADP systems and/or network (CIS) storing, processing or transmitting information classified NATO COSMIC TOP SECRET, and/or Special Category information;
b) ADP systems and/or network (CIS) storing, processing or transmitting information classified NATO SECRET, where:
    (i) ADP system and/or network (CIS) is interconnected with another ADP system and/or network (CIS)
    (ii) ADP system and/or network (CIS) has a potential user population which cannot be specifically defined.

263. The evaluation and certification processes shall be carried out in accordance with the approved principles/directives, by independent and impartial teams of technically qualified and appropriately cleared personnel, acting on behalf of SAA. This Agency shall be involved in the selection of

the appropriate teams to carry out the evaluation and certification processes.

264. The teams are formed of SAA specialists, or its nominated representatives, or specialized NATO bodies members.

265. The evaluation and certification processes shall establish the extent to which the design and implementation of a particular ADP system and/or network (CIS) meets specified security requirements, as stated in the SSRS. Relevant sections (paragraphs) of the SSRS may require modifying or updating after evaluation and certification. The evaluation and certification processes shall commence at ADP system and/or network (CIS) specification stage and continue through the implementation cycle.

266. The degree of evaluation and certification processes involved may be lessened when ADP systems or network (CIS) are based on already existing nationally evaluated and certified computer security products.

267. For all ADP systems and/or network (CIS) storing, processing or transmitting information classified NATO CONFIDENTIAL and above, CISLOA establishes control procedures, which shall ensure that all ADP systems and/or network (CIS) changes are reviewed for their security implications.

268. The types of change that would give rise to re-accreditation, or that require prior approval of the SAA, shall be clearly identified and stated in the SSRS (see paragraph 193). After any modification, repair, or failure, which could have affected the security features of CIS, CISLOA shall ensure that a check is made for the correct operation of the security features. Continued accreditation of the CIS shall depend on the satisfactory completion of the checks.

269. All ADP systems or network (CIS) storing, processing or transmitting information classified NATO CONFIDENTIAL and above, shall be inspected or reviewed on a periodic basis by the SAA. In respect of ADP systems or network (CIS) storing, processing or transmitting NATO COSMIC TOP SECRET or Special Category information, the inspections shall be carried out not less than once annually.

270. Microcomputers/ Personal Computers (PCs) with fixed hard disks (or other non-volatile storage media), operating either in stand-alone mode or as networked configurations, and portable computing devices with fixed hard disks, are considered as information storage media in the same sense as other removable computer storage media.

271. This equipment shall be granted the level of protection for access, handling, storage and transportation, according to the highest classification level of information ever stored or processed within it, until downgraded or de-classified in accordance with approved procedures.

272. The use of privately-owned removable computer storage media, software and ADP hardware with a storage capability are prohibited for storing, processing and transmitting information classified NATO CONFIDENTIAL and above. For NATO UNCLASSIFIED and NATO RESTRICTED information, the appropriate national regulations shall be applied.

273. Privately-owned hardware, software and removable media are forbidden to be brought into any area where NATO classified information is stored, processed or transmitted without the permission of the head of the organization.

274. Use of contractor-owned ADP equipment and software in organizations for official NATO work is allowed with the approval of the head of the organization. The use of the ADP equipment and software provided by other national institutions may also be permitted; in this case the ADP equipment shall be brought under the control of the appropriate organization's inventory. In either case, if the ADP equipment is to be used for storing, processing or transmitting NATO classified information, the appropriate SAA approval must be obtained.

275. The marking for special designation information, is currently applied to classified information with limited distribution and/or special handling, in addition to the character assigned by the security classification (for example ATOMAL, US-SIOP-ESI, Crypto, EXCLUSIVE FOR etc.)

276. The definitions provided in the following paragraphs are important concepts for the NATO specific terminology and may, in some cases, differ from national definitions.

277. *Information in Electronic Format* represents texts, data, images, sounds recorded on magnetic, optic or electric media, or transmitted as current, voltage or electromagnetic field, in open space or in communication networks.

278. *Two Men Rule* represents the mandatory character of cooperation of two persons in fulfilling a specific task.

279. *ADP System and/or Networks (CIS) security* represents the application of security measures to ADP systems or networks (CIS), in order to prevent or deny both retrieving and/or modification of NATO

classified information stored, processed or transmitted through ADP System and/or networks (CIS) by means of interception, alteration, destruction, unauthorized electronic access, as well as by denial of services/functions through specific means.

280. *ADP System and/or Networks (CIS) security assurance* means implementing a set of combined measures: ADP system and/or network (CIS) specific security measures (i.e. at computer level), communication security, and also procedural, physical, personnel and document security measures.

281. *Computer Security (COMPUSEC)* consists in the application of hardware, firmware and software security features to a computer system in order to prevent unauthorized disclosure, handling, and modification /deletion of information or unauthorized denial of service.

282. *Computer Security Product* represents a computer security item incorporated into an ADP system and/or network (CIS) for use in enhancing or providing for confidentiality, integrity, authentication, non-repudiation or availability of information stored, processed or transmitted.

283. *COMMUNICATION SECURITY (COMSEC)* represents the application of security measures to telecommunications in order to protect messages within a telecommunication system, which might be intercepted, studied, analyzed and then, by restoration, can conduct to classified information disclosure.
COMSEC is a complex procedure set including:

a) transmission security measures;
b) emission security measures (TEMPEST);
c) cryptographic measures;
d) procedural, physical, personnel and document security measures;
e) COMPUSEC measures.

284. *TEMPEST* represents measures of testing and ensuring the security against leakage of information through parasite electromagnetic emissions.

285. *EVALUATION* consists in a detailed technical and functional examination of the security aspects of an ADP system and/or network (CIS) or security products, by an appropriate authority.

(1) Through the evaluation process, the presence of the required security features (functions) and the absence of compromising secondary effects resulting from security features implementation are verified, and the overall functionality of the security system is estimated;

(2) The evaluation determines the extent to which the specific security requirements of an ADP system and/or network (CIS) are satisfied. It also assesses the security performances of the computer security products

installed within CIS and establishes the trust level of the ADP system and/or network (CIS) or the implemented computer security products.

286. *CERTIFICATION.* At the end of the evaluation stage, a finding document is issued, at which an analysis document is attached, reporting the evaluation and its results. This document mentions the extent to which the verified ADP system and/or network (CIS) meet the security requirements and the extent to which the computer security products meet the pre-defined security claims.

287. *ACCREDITATION* is the stage for granting the authorization and approval to an ADP system and/or network (CIS), to process NATO classified information in its operational environment.
The accreditation stage shall be made after all appropriate security procedures have been implemented and a sufficient level of system protection has been achieved. Accreditation is mainly performed on the basis of the SSRS, including the following:

(a) a justifying statement upon the objective of system accreditation; other details included: classification level(s) of information to be processed and handled, security mode(s) of operation being proposed;
(b) a risk management review (mode of risk treatment / accounting/solving) identifying the threats and vulnerabilities, as well as their adequate countermeasures;
(c) a detailed description of the security features and proposed procedures intended for ADP system and/or network (CIS). This description shall represent the essential element for completing of the accreditation process;
(d) a plan for the implementation and maintenance of the security features;
(e) a plan for carrying on security test, evaluation and certification stages, regarding ADP system and/or network (CIS);
(f) a certificate and, where required, supplementary elements of accreditation.

288. *ADP SYSTEM* represents an assembly of interdependent elements including: computer equipment, basic and application software, methods, procedures, and if necessary, personnel – thus managed in order to accomplish storing, automatic processing and transmitting electronic information within the system. Such systems may be used in specific applications for industrial, economic, military, research, design and administrative domains.

(1) For establishing the boundaries an ADP System is extended up to, this is defined as an assembly of elements under coordination and control of a single CISLOA;
(2) An ADP System may contain subsystems, some of them ADP System themselves.

289. *ADP SYSTEM SPECIFIC SECURITY FEATURES* represent:
- hardware / firmware / software functions and attributes;
- operating procedures and operating modes;
- accountability procedures;
- access control;
- definition of the ADP System operating area;
- definition of the remote terminal / workstation operating area;
- restrictions imposed by management policy;
- physical structure and devices;
- personnel and communications control means.

All these are needed to provide an acceptable level of protection for classified information to be stored or processed in an ADP System.

290. *DATA TRANSMISSION NETWORK (DTN)* represents an assembly of interdependent elements, including: communication equipment and devices, computer hardware and software, data transmission / reception methods and procedures, and for network control. If necessary, the involved personnel are included. All these are organized in such a manner to ensure the accomplishment of the electronic information transmission functions between two or more ADP systems (CIS), or to permit the interconnection with other Data Transmission Network. DTN may use the services of one or more communication systems; more DT Networks may use the services of the same communication system.

291. *SPECIFIC SECURITY FACILITIES FOR DTN* include the network together with all additional components and facilities associated with that network (network communication facilities, mechanisms and procedures for security identification and labeling, access controls, programs and procedures for control and technical revision) needed to provide an acceptable level of protection for classified information.

292. *COMMUNICATION INFORMATION SYSTEM (CIS*) represents, by structure, a connection of at least one ADP System and/or a DTN. Using CIS, information is stored, processed and transmitted in electronic format.

293. *ADP SYSTEM AREA* represents a working area, containing one or more operating computers, their local peripheral and storage units, control units and dedicated network and communication equipment. *ADP System area* does not include the separate area in which remote peripheral

devices, terminal or workstations are located, even though those devices are connected to the central computer equipment of ADP System area.

294. *REMOTE TERMINAL / WORKSTATION AREA* represents an area – separated from *ADP System area* – including:

- local peripheral equipment or terminals associated to the central computer equipment;
- remote workstations;
- DTN communication equipment

J. SECURITY STRUCTURE/OFFICER

295. A security structure/officer will be designated at the level of each autonomous administrative authority or ministry and the subordinated structures handling NATO classified information. It will implement the security measures and organize the activity of protection of NATO classified information. The number of personnel in this structure shall be dimensioned on the amount of information.

296. Designation of a security structure/officer is mandatory in all institutions, companies, private or public enterprises which, by the nature of their activity or due to the let contracts, agreements or understandings, handle NATO classified information.

297. The security structure/officer is the point of contact between the institution and NSA.

298. The security structure/officer is appointed by the head of the institution and is directly subordinated to him. The security structure/officer is responsible for the implementation of the security norms and procedures for the protection of NATO classified information within that institution, as well as the subordinated structures, for each security field regulated by the NSA: security organization, physical security, personnel security, document security, industrial security and INFOSEC.

299. The responsibility for implementing the regulations regarding the protection of NATO classified information rests with the head of the institution. The security structure/officer is his main collaborator and executive component.

300. In accordance with the regulations regarding access to NATO classified information, the personnel from the security structure shall hold a type A personal security clearance certificate at the highest level of classification of the handled NATO classified information.

301. The tasks of the security structure/officer are:

General tasks:

a) coordinates the activity of the CNRS within that institution and the subordinated structures;
b) draws up internal norms to implement the regulations regarding protection of NATO classified information;
c) monitors the implementation of the internal security norms for NATO classified information, as well as the way these norms are observed within the institution;
d) draws up the security plan for the protection of NATO classified information within the institution;
e) provides advice to the head of the institution on each aspect concerning security of NATO classified information;
f) informs the head of the institution on the vulnerabilities, risks and breaches of security and suggests measures in such situations.

Tasks on personnel security:

a) ensures implementation of the internal norms regarding personnel security;
b) initiates the process of request for the issuance of security clearance certificates, at the order of the head of institution;
c) provides the questionnaires for the appropriate level of access requested to the person who needs to be issued a security clearance certificate;
d) provides assistance for filling in the security questionnaires, observing the deadline for sending the request;
e) provides necessary support to the institutions authorized to conduct security vetting upon persons who will have access to NATO classified information;
f) keeps up-to-date record of all persons in the institutions who have access to NATO classified information, a copy of the security clearance certificate, and takes the necessary measures to revalidate or withdraw the security clearance certificates;
g) reassesses periodically and updates the internal norms for the implementation of the regulations regarding the protection of NATO classified information.

Tasks on document security

a) coordinates and monitors the implementation of internal norms on the security of NATO classified documents within the institution;
b) inspects the activity of the CNRS as to the way of handling and managing NATO classified documents;
c) prepares and transmits to the NSA the request and necessary documentation for the establishment of a CNRS within the institution.

Tasks on physical security:

a. establishes the physical security measures to control access in security areas, in order to prevent unauthorized access;
b. performs checks on the security conditions of the places, rooms, offices and containers where NATO classified information is handled or stored;
c. adopts the necessary measures to ensure an appropriate physical protection level in all rooms where NATO classified activities take place;
d. prepares and conducts inspections on physical security measures within the CNRS in its area of competence and informs the head of institution on the found vulnerabilities;
e. performs on the spot checks upon the physical protection systems;
f. establishes the cooperation plan with other units responsible for ensuring the physical protection.

The tasks on INFOSEC are provided in Chapter I - INFOSEC.

The tasks on personnel training are provided in Chapter L – "Personnel Training".

K. CONTROL ACTIVITY

302. Control is the activity of checking the way each CNRS ensures the protection of NATO classified information.

303. The control activity will be performed in a planned manner, based on the Overall Control Plan.

304. All structures and persons handling NATO classified information will be included in control programs and will be notified as to the control objectives.

305. Each control activity shall finish with a report drawn up by the team performing the control.

306. The control activity shall be meant to identify, eliminate and counter any security risks that may lead to compromise, destruction or theft of NATO classified information.

307. The control activity aims at the security structure/officer, CNRSs and personnel with access to NATO classified information.

308. The results of the control activity will materialize in a set of measures meant to ensure the operationalization and improvement of the organizational and functional framework, at all structures and levels of activity dealing with the protection of NATO classified information.

309. NSA shall organize and coordinate the control activity at national level.

310. NSA shall check on the implementation of measures and recommendations necessary to achieve the undertaken objectives at the level of subordinated CNRSs.

311. The Coordination Board shall designate the members of the control and inspection team, with the approval of the NSA President.

312. The coordinating role of the NSA shall be performed by drafting the Overall Control Plan, and by undertaking the responsibility at national level as to the requests and inspections conducted by the NOS in Romania.

313. NSA shall integrate the proposals submitted by the subordinated security structures and those made by the NOS in order to establish, plan and perform the control topics. Following the inspections and whenever facts or malfunctions are established that may constitute security risks for the protection of classified information, NSA shall inform the NOS, in due time, and shall simultaneously take action, together with the relevant security structures in order to counter/lower and assess the security incidents.

314. NSA shall perform inspections in accordance with the Overall Control Plan at the subordinated CNRSs and shall supervise such activities conducted by all CNRSs in the National Registry System.

315. Annually or whenever necessary, NSA shall make an assessment of the inspections results, the way of implementing the measures necessary to remedy the deficiencies and the practical manner of making the activity of protection of NATO classified information more effective.

316. Based on the Overall Control Plan, each CNRS shall develop its own Specific Control Plan, addressing in a differentiated way to the subordinated CNRSs. The control topics, planning and reporting will be recorded in the Overall Control Plan, being adjusted to fit the conditions of each CNRS.

317. NSA shall be informed on the post-control established results, propositions and measures for making the protection of NATO classified information more effective.

318. In case security risks are found, as to the compromise, disclosure, destruction or theft of NATO classified information, a security inquiry will be performed and the results will be notified to the NSA. The members of the inquiry team will be designated by the head of institution.

319. CNRSs shall keep record of all performed inspections, the inspection topics and the inspected personnel.

320. The Overall Control Plan is drawn up annually, by the NSA, in accordance with its relevant tasks and the suggestions made by the NOS.

321. The fields, topics, stages and forms of control are integrated in this Plan and are the basis on which the Specific Control Plan will be drafted by the subordinated structures.

322. This Plan will be approved by the NSA President and the Coordination Board, and the responsibility of implementing the measures and conducting the planned activities rests with the Technical Secretariat.

323. Based on the Overall Control Plan, the security structure/officer shall develop its own Specific Control Plan, addressing in a differentiated way to the subordinated CNRSs.

324. The Specific Control Plan will be approved by the head of the institutional structure where the CNRS functions.

325. Within two weeks since the completion of the activities provided in the Specific Control Plan, the security structure/officer shall submit to the NSA a report on the inspection results.

326. The control activities may be planned and announced, planned and not announced, unplanned and for emergency situations. They may be performed under the following form:

1. Overall controls – with a purpose to check the activity of protection of NATO classified information from the organizational, structural and functional point of view;
2. Topic controls performed on the basis of specific topics and aiming at one or more fields of the protective security activity and/or training and security education programs.
3. Emergency controls meant to strictly check and resolve incidents or express requests to the NSA as a result of identifying a security risk.

L. PERSONNEL TRAINING

327. The training of the personnel is a form of the security education compulsory for all persons who handle/will handle NATO classified information. It represents the specific activity of information and training in the field of NATO classified information protection. Persons employed by institutions where NATO classified information is handled and who have been issued a security clearance certificate will be trained before starting their activity.

328. The training activity will be carried out in a planned manner, permanently, in order to prevent, counter and eliminate the security risks and threats to NATO classified information security.

329. Personnel training will be conducted differentiated, depending on the personnel tasks and the level of security clearance.

330. Each training form will be recorded in the individual training form of the person.

331. Personnel training aims at correct understanding and learning of the security standards, as well as the way of effectively implementing the measures for the protection of NATO classified information, in order to eliminate the malfunctions.

332. In the framework of the Overall Personnel Training Plan, NSA shall establish training topics, on fields, forms and methods of conducting the training activities, depending on the personnel tasks and the level of the security clearance. This will be done in cooperation with the security structures from institutions handling NATO classified information.

333. NSA will cooperate with the NOS in order to establish the Overall Training Plan.

334. NSA is responsible for carrying out the public information and security education. These will aim at different target groups and will have the purpose of raising awareness and level of information on the need to protect NATO classified information, at the level of the entire society.

335. The security structure/officer has a coordinating role in drafting, implementing and inspecting the way personnel training programs are implemented.

336. The security structure/officer shall draft the Specific Training Plan, which is part of the Overall Training Plan. Based on the Specific Plan, it will pursue specific training activities at the level of the institutional structure and its subordinated departments.

337. Periodically, the security structure/officer shall inform the NSA on the pursued training forms and shall transmit a list of the trained personnel.

338. The security structure/officer shall keep record of all personnel participating in training activities organized by NATO, security structures of the Alliance or at national level.

339. The Overall Training Plan is drafted and approved by the NSA, based on the suggestions made by the security structures/officers, the domestic or international bilateral cooperation agreements and the recommendations made by the NOS. It is drafted annually and released to all institutional structures.

340. The Specific Personnel Training Plan is drafted at the beginning of the year, by each institutional structure, adjusted to its own conditions, based on the provisions stipulated in the Overall Training Plan. The specific Training Plan shall be approved by the head of the institutional structure.

341. Every three months, the institutional structures shall inform the NSA on the results of implementing the Specific Training Plan and shall submit proposals of possible activities to be included in the Overall Training Plan.

342. The general training entails the objectives, tasks and responsibilities resting with each structure in order to implement the measures for the protection of NATO classified information. The general principles of protecting NATO classified information, ways of implementing these standards, forms and methods of making them consistent with relevant NATO requirements are presented at this level.

343. The specific training is conducted based on the need-to-know principle, the specific field of activity, the performed tasks and the level of security clearance.

344. Individual training shall be performed compulsory by all personnel handling NATO classified information, in accordance with their tasks.

345. The general and specific topics may be presented during lessons, briefings, lectures, symposia, panel talks, working groups, seminars, workshops, meetings, discussions, completed with tests and checks on the level of knowledge accumulated.

346. The training activities are carried out according to the Overall Training Plan, by the security structures, as well as other authorities, institutions, governmental organizations, NGOs and other bodies authorized by the NSA to conduct such activities, based on signed protocols.

347. Common training programs shall be pursued based on the agreements concluded between NSA and similar international institutions, as well as authorities, governmental organizations, NGOs, bodies and structures with tasks on protection of NATO classified information.

348. Each institution shall designate the persons who will participate to such training forms and will request permission for participation through the security structure. In case of training organized by the NSA, the request will be send to the NSA by the security structure.

349. The form of training will be organized by the experts of the NSA Technical secretariat, according to the topics provide in the Overall Personnel Training Plan.

350. Annually or whenever necessary, NSA shall organize training sessions for the security officers and the personnel from the CNRSs.

351. The training sessions shall be organized by the security structure/officer, according to the topics from the Specific Training Plan. Upon request of the security structures/officers, NSA will provide assistance.

Annexes

R O M A N I A

RESTRICTED
(when filled in)
Copy no. ___

……
Ministry

……..
Requesting institution

No. _____ date _____

NATIONAL SECURITY AUTHORITY

To Mr. ……..
President of the National Security Authority

We request initiation of the vetting procedure for the issuing of the security clearance certificate for:

Name:
First name:
DoB:
PoB:
I.D.
Series: ☐ No: ☐
Issued at: ☐

Type A certificate of security clearance:

Level: CONFIDENTIAL ☐ SECRET ☐ TOP SECRET ☐

Type B certificate of security clearance:

Level: CONFIDENTIAL ☐ SECRET ☐ TOP SECRET ☐

Activity, place:

Period:

Passport type: SERVICE ☐ DIPLOMATIC ☐

Series: ☐ Nr: ☐ Issued at: ☐

Please find attached the vetting forms no._____ of___.___.___

HEAD OF THE REQUESTING INSTITUTION

Name:

Signature:

Date:

L.S.

R O M A N I A

RESTRICTED
(when filled in)
Copy no. ……

NATIONAL SECURITY AUTHORITY

No. _____ of _____

To Mr. ……

We request initiation of the vetting procedure, based on the request no._____of_____ made by _____ for the issuing of the certificate of security clearance for:

Name:
First name:
DoB:
PoB:

I.D. Series No:

Issued at:

Type A certificate of security clearance:

Level: CONFIDENTIAL ☐ SECRET ☐ TOP SECRET ☐

Type B certificate of security clearance:

Level: CONFIDENTIAL ☐ SECRET ☐ TOP SECRET ☐

Activity, place:

Period:

Passport type: SERVICE ☐ DIPLOMATIC ☐

Series: Nr Issued at:

Please find attached the vetting forms no. _____of___.___.___

PRESDIDENT OF THE NATIONAL SECURITY AUTHORITY

Name:

Signature:

Date:

L. S.

R O M A N I A

RESTRICTED
(when filled in)
Copy no. ___

……
Ministry

……..
Requesting institution
No. _____ date _____

NATIONAL SECURITY AUTHORITY

To Mr. ……..
President of the National Security Authority

This is to notify initiation of the vetting procedure for the issuing of the security clearance certificate for:

Name:
First name:
DoB:
PoB:

I.D. Series: ____ No. _____

Issued at: _____

Type A certificate of security clearance:

Level: CONFIDENTIAL ☐ SECRET ☐ TOP SECRET ☐

Type B certificate of security clearance:

Level: CONFIDENTIAL ☐ SECRET ☐ TOP SECRET ☐

Activity, place:

Period:

Passport type: SERVICE ☐ DIPLOMATIC ☐

Series: ____ Nr: _____ Issued at: _____

Please find attached the vetting forms no. _____of___.___.___

HEAD OF THE REQUESTING INSTITUTION

Name:

L. S.

Signature:

Date:

Nr. 1234

NATIONAL SECURITY AUTHORITY

TYPE A CERTIFICATE OF SECURITY CLERANCE

1. Certification is hereby given that:

Full Name:

Paul – Doru STĂNESCU

Date and Place of Birth:

December 06, 1973, Constanța, Constanța County

has been granted a personnel security clearance by the Government of: ROMANIA – National Security Authority **in accordance with the provisions of the Security Arrangements between NATO and ROMANIA and is, therefore, declared suitable to be entrusted with information classified up to and including SECRET**.

2. The validity of this certificate will expire not later than **14.12.2004**.

Signed: **MIHNEA MOTOC**

Title: President *Official Government Stamp*

Date: 14.12.2001

Nr. 2345 **NATO/EAPC/PfP UNCLASSIFIED**

CERTIFICATE OF SECURITY CLEARANCE

Issued by
NATIONAL SECURITY AUTHORITY OF ROMANIA

Date and Place of Issue
14.12. 2001, Bucharest

Valid until
01.01.2002 - 30.11.2002

This is to certify that:

Full Name
Paul – Doru STĂNESCU

Date of Birth
December 06, 1973

Place of Birth
Constanța, Constanța County

***Where employed*:**
Ministry of National Defence

Purpose and Duration of Visit
Appointed to the Defence Cooperation and Partnership Directorate, NATO HQ, Bruxelles, Belgium
01.01.2002 – 30.11.2002

***Holder of Passport/Identity Card No*. P - 034567**
***Issued at* Ministry of Foreign Affairs**
***Dated*: 07.10.1999**
has been cleared for access to NATO/EAPC(PfP) information classified up to and including **NATO/EAPC(PfP) SECRET** in accordance with current NATO security requirements and has been briefed accordingly by **National Security Authority of Romania**.

Signed: **MIHNEA MOTOC**

Title: President *Official Government Stamp*

Date: **14.12. 2001**

R O M Â N I A
RESTRICTED

(when completed)

.....
Institution

Copy no. ……

No. _____ from _____

COURIER CERTIFICATE NO. ……

FOR THE INTERNATIONAL HAND CARRIAGE

OF CLASSIFIED DOCUMENTS,

EQUIPMENT AND/OR COMPONENTS

This is to certify that the bearer:
Mr./Ms.:
_____
Born on: (day/month/year) __/___/_____, in (country):
_____
Holder of passport/identity card no.: (number)
_____
Issued by: _____on: (day/month/year)
___/___/____
Employed with: (company or organization)_____
Escort:
Mr./Ms: _____
Born on: (day/month/year) __/___/_____, in: (country)_____
Holder of passport/identity card no.: (number)
_____
Issued by: _____ on: (day/month/year)
___/___/____
Employed with: (company or organization)_____

Is authorized to carry on the journey detailed below the following consignment:

No	KIND OF DOCUMENT/MATERIAL	DOCUMENT/MATERIAL SERIES	MENTIONS

ITINERARY:

From (originating country):_____

To (country of destination):

_____

Through:

_____

Authorized stops:

1. _____
2. _____
3. _____
4. _____
5. _____

Date of beginning of journey: ___/___/_____

Data of ending the journey: ___/___/_____

Signature of company's Security Officer

_____

(name)

Signature of the Head of the company

_____

(name)

Company's stamp

I declare in good faith that, during the journey covered by this "Courier Certificate", I am not aware of any occurrence or action, by myself or by others, which could have resulted in the compromise of the consignment.

Courier's Signature: _____

Companion's Signature: _____

Witnessed by: _____
(Company Security Officer's signature)

Date of return of the "Courier Certificate": ___/___/_____