1. Basic Information

1.1 CRIS Number: BG 2005/017-586.02.01
1.2 Title: Further Strengthening of the Administrative Capacity of Bulgarian Police and Providing Conditions for Application of the Classified Information Protection Act in the Public Administration of the Republic of Bulgaria – a Stage in the Protection of EU Classified Information.
1.3 Sector: Justice and Home Affairs, Sub-sector: Police/Crime
1.4 Location: Republic of Bulgaria, Communication and Information Security Directorate (CISD) – Ministry of Interior (MoI)
1.5 Duration: 1,5 –year Twinning with an investment component

2. Objectives

2.1 Overall Objective(s):

To further strengthen the security unit in the Ministry of Interior responsible for the implementation of the classified information protection policy of the Republic of Bulgaria and modernize procedures (SOPs – standard operating procedures), organisation and management systems, and equipment to authorise and monitor access to classified information and prevention of unauthorized access to it in line with Agreement between the EU and the NATO on the security of information; Security Regulations of the Council of the EU - Basic Principles and Minimum Standards of Security Protection of Information Handled in Information Technology and Communication Systems; Council Decisions of the Commission of the European Communities and ISO/IEC 17799, BS 7799 Part 1 and Part 2, Common Criteria ISO 15408.

2.2 Project purpose:

To achieve a higher effectiveness of police activities by adoption and implementation of the best practices in prevention and protection of Automated Information Systems (AIS) and public administration networks against unauthorised access, hacking, fraudulent manipulation, data protection infringements; further modernization and rationalization of the training system, putting in place organizational, administrative procedures and using technical, informational technological and other equipment to prevent any crime activities in the Republic of Bulgaria at obtaining unauthorized access to classified information.

2.3 Accession Partnership (AP) priorities, Catalogue of Main Administrative Structures for the Implementation of the Acquis, Road Map for Bulgaria, National Program for the Adoption of the Acquis (NPAA), updated National Strategy for Combating Crime, Multi-annual Phare Programming Document

EU Common Position on Accession and Contracting Principles

- EU underlines the important principle of sustaining responsible, reliable and coordinated police organisation;
- EU recalls the need for such organisation to be functional for the purpose of comprehensive and precise Acquis application by the accession date at the latest;
- The latter suggests a practical and effective cooperation and information flow among the institutions in this field, computer searching capability, initial and follow-up training
adjusted to the needs of combating specific crimes, as well as national statistical instruments for measuring crime growth and combat results;

**Accession Partnership**
- Implementation of the Strategy for Combating Crime with special attention to different forms of cross-border and organized crime like drug traffic, human traffic etc. and to coordination and practical cooperation among law-enforcement authorities;
- Strengthening of police and judicial capacity (number of officers, appointment, training, technical equipment) for further combat against organized crime, drug traffic, corruption, and for reinforcement of police and customs authorities and ensuring better coordination.

**Catalogue of Main Administrative Structures for Acquis Implementation**
Each structure needs sufficient staff, infrastructure and equipment for performing its functions effectively. This suggests the availability of an integrated computer system for investigation, to which the relevant police authorities have access, national statistical instruments for measuring crime and the number of closed cases. The guaranteed coordination and cooperation among police and other related authorities is of utmost importance.

Member Countries must have institutions in line with EU standards. They have to implement measures for combating organized crime, terrorism and drug traffic. Member Countries must have the necessary technical equipment for detecting fake and forged documents.

**Road Map for Bulgaria**
In the Road Map for Bulgaria, Chapter 24: Cooperation in Justice and Home Affairs, it is noted that Bulgaria should concentrate its further efforts on substantially reinforcing the capacity of its judicial and law-enforcement authorities and improving their cooperation. Special attention should be paid to the authorities dealing with fraud, corruption, money laundering, observation of the Schengen Agreements, police coordination and anti-drug policy. Bulgaria should concentrate its further efforts on administrative capacity reinforcement and methodology modernisation and an overall improvement of data quality and completeness. Concrete mid-term steps are the strengthening of administrative capacity and especially further training and development of statistic administration employees and informational technological capacity, specifically in regional offices.

**National Program for the Adoption of the Acquis**
- Elaboration of basic rules for exploitation of communication and information systems in compliance with EU standards and requirements.

**Updated National Strategy for Combating Crime**
(adopted by the National Assembly of the Republic of Bulgaria on 30 Jan 2004)
- Improvement of effectiveness in combating crime by use of information technologies and systems in compliance with EU requirements, including the introduction of bio-metric indices for identification of foreigners;
- Expansion of police cooperation with EU countries in combating organized crime;
- Elaboration of national statistical instruments in line with EU standards for measuring crime and detection of criminal acts;
- Development of a system for protection of classified information and information technologies, carriers and means;

**Multi-annual Phare Programming Document**
• Priorities for Sub-sector Crime/Police, respectively the main activities of this Sub-sector, result from the specific measures, envisaged in the key national strategies for the Sub-sector, which are to be supported by Phare: Public Administration Modernisation Strategy, Strategy for Combating Crime, Anti-drug Strategy. These strategic documents of Bulgaria aim as a whole the combat against conventional, organized and cross-border crime, money laundering, drug and pre-cursor control, human traffic, protection of personal data and classified information against criminal acts.

2.4 Contribution to National Development Plan (and/or Structural Funds Development Plan/SDP)

NA

2.5 Cross Border Impact

NA

3. Description

NOTE: This Project fiche corresponds to recommendations of the Regular Report 2004 – ‘Bulgaria needs to continue to strengthen the security unit in the Ministry of Interior' and ‘Further efforts are needed as regards the modernisation of training equipment’.

3.1 Background and justification:

The Ministry of Interior Act (MoIA) – article 124, paragraph 1, point 1 and 2, and the Classified Information Protection Act (CIPA) – article 14, envisage the following major priorities in the work of the Communication and Information Security Directorate:
1. Cryptographic protection of classified information;
2. Issuance of security certificates of AIS or networks working with classified information;
3. Coordination and control of the protection against spurious electromagnetic emissions from technical devices processing, storing and transmitting classified information;
4. Implementation and supervision of training courses in application of cryptographic methods and means by officers who have obtained permission for access to classified information.

With respect to these functions CISD started making a laboratory for measuring electromagnetic emissions from technical devices, which process, store and transmit classified information, as well as testing laboratory for encryption devices and their cryptographic algorithms. CISD also began the construction of a modern auditorium for training courses in application of cryptographic methods and means by officers who have obtained permission for access to classified information. The possibility for creating a mobile laboratory is being considered at the moment since it is necessary for inspecting the security measures in issuing security certificates of AIS or networks working with classified information.

Cryptographic protection of classified information includes testing of cryptographic devices and their cryptographic algorithms
In its capacity of a Cryptographic Security Authority of the Republic of Bulgaria under the Regulation on Cryptographic Security of Classified Information CISD:

1. Implements the national policy on cryptographic security of classified information according to CIPA, this Regulation and other bylaws on classified information protection;
2. Provides guidance and recommendations on all cryptographic security aspects;
3. Evaluates and approves cryptographic methods and means for classified information protection;
4. Participates in the overall evaluation of the security of cryptographic networks and the approval of their exploitation;
5. Generates and distributes cryptographic keys for the protection of classified information in the cryptographic networks of the Republic of Bulgaria;
6. Participates in the overall evaluation of the security of systems for automated generation and distribution of keys and in the approval of their exploitation;
7. Coordinates and controls the exploitation, production and import of means for cryptographic protection of classified information;
8. Conducts training in cryptographic security and issues permissions for exploitation of cryptographic means;
9. Provides methodological instruction to cryptographic security officers;
10. Approves and controls cryptographic security training conducted by other organizational units;
11. Draws written statements in cases of cryptographic security compromise;
12. Keeps a record of approved cryptographic means and issues passports to all individually tested cryptographic means;

With respect to point 3, 4, 5, 6, 12 and 13 CISD began the construction of a testing laboratory for simulation of actual working conditions of a large variety of cryptographic communication devices. In view of the variety of these devices and the fast developing technologies in the field it is important for the technical and software equipment of the testing laboratory to support a lot of network protocols and transmission media for the purpose of improving the effectiveness, speed and quality of work. Another factor determining the need for a testing laboratory is the existence of standard encryption devices which are necessary for testing new or repaired devices on the territory of the laboratory.

At present due to the lack of certain modules of the existing devices (hardware protocol analyzer) part of the incoming equipment cannot be tested. Another problem is the real-time operation of these devices. The solution to these and other problems related to the technical equipment of the testing laboratory requires the purchase of a new hardware protocol analyzer, which is substantially better in terms of real-time analysis and data processing than high-speed standards like GigaBit Ethernet, STM-1e/EC-3 or STM-4/OC-12, as well as the other standards of the OSI model of communication protocols. Each transmission medium needs specific active communication devices as concentrators, routers, testers etc. The dynamic development of the field creates a necessity for training specialists to handle and analyze the new protocols.

The process of issuing security certificates of AIS or networks working with classified information includes accreditation of these AIS or networks

In its capacity of a Security Accreditation Authority for AIS or networks, under the Regulation on the General Binding Conditions for Security of AIS or networks which produce, process, store and transmit classified information, CISD performs the following activities:

1. Provides guidance and recommendations on the security of AIS or networks;
2. Recommends standards and means, which can be used in AIS or networks for protection of classified information;
3. Approves the security documents of AIS or networks;
4. Makes an overall evaluation of the security of AIS or networks;
5. Issues security certificates for AIS or networks;
6. Establishes the conditions for additional or new accreditation of AIS or networks;
7. Coordinates and controls the protection against parasitic electromagnetic emissions from technical devices processing, storing and transmitting classified information;
8. Conducts training of security officers for AIS or networks;
9. Keeps a record of certified AIS or networks.

Activities under point 2, 4, 6 and 7 necessitate the equipment of a mobile laboratory for network analysis and monitoring. It will enable the inspection of AIS or networks on the ground during their construction or accreditation. In view of the large variety of exploited networks and the fast developing technologies in the field it is important for the technical and software equipment of the laboratory to support a large variety of network protocols and transmission media. Security evaluation, especially of functioning AIS or networks, involves-establishing (by hardware and software instruments) the actual number of terminals and users, as well as the existence of links to other networks (public networks or networks processing or transmitting classified information), and TEMPEST zoning. Equally important is the capacity of the devices and the automatic measurement software, the user-friendly interface and the drawing of comprehensible reports. During the accreditation process AIS must be tested for their own electromagnetic emissions, as well as the premises and buildings in which they will be located. The construction of a mobile laboratory requires the purchase of a van equipped with the following devices: network analyzer, modules for connection with different types of networks, analysis and monitoring software and portable computer and TEMPEST zoning. The measurement of electromagnetic emissions requires the purchase of a generator up to 40 GHz, spectrum analyzer up to 40 GHz, two radio sets enabled to connect with PCs, two portable computers, two sets of calibrated antennas up to 40 GHz, powerful amplifier up to 40 GHz and pre-amplifier up to 40 GHz.

The coordination and control of the protection against spurious electromagnetic emissions from technical devices processing, storing and transmitting classified information involves tests for electromagnetic emissions in an anechoic chamber

In the CISD have equipment of a RFD-F/A-100 anechoic chamber for measuring electromagnetic emissions. The chamber has a turn table and antenna mast allowing automatic change of polarization during measurement. The measurements are taken remotely from outside by a laboratory for microwave measurements, whose construction in front of the chamber has already started. The process is automated with the help of a computer operating a control panel for the table and the mast inside the chamber and the spectrum analyzer outside. Special software has been elaborated for the purpose and the process is controlled by GPIB interface. The software can also control a cable measuring generator. The laboratory has a set of calibrated antennas from 100 Hz to 18 GHz.

Technical measurements are taken at the preliminary request of different departments throughout the country or MoI departments. After the measurements the technical devices are provided with qualification and recommendations for their exploitation.

The equipment in use at present is not specialized for measuring electromagnetic interferences. It has a lower sensitivity (max 115 dBm) and its brand is 10 years old. At present firms offer non-specialized spectrum analyzers with 150 dBm sensitivity, as well as specialized systems for measuring electromagnetic interferences and electromagnetic compatibility, which include a highly sensitive receiver, calibrated antennas, cables, pre-amplifiers and powerful amplifiers and specialized software for measurement control and reading of results. The improvement of
sensitivity and quality demands the purchase of a high precision system with specialized software with the necessary accessories.

Precision is achieved by regular measurement of cables, amplifiers and antennas for VSWR, amplification and losses and on the basis of these results the algorithms for final measurements are corrected. For this purpose the laboratory needs a microwave vector analyzer (Network Analyzer to 40 GHz) with accessories, and two sets of calibrated antennas up to 40 GHz, powerful amplifier up to 40 GHz and pre-amplifier up to 40 GHz.

The police service modernisation and changes in regulation in compliance with EU standards require permanent rise in the professionalism of police officers and adoption of modern practices and procedures for classified information protection.

The specialists working in the laboratory are well qualified but they need training courses in exploiting specialized measurement equipment, as well as introductory knowledge of EU standards in this sphere with the aim of putting them to practice.

Training in exploitation of cryptographic methods and means of officers who have obtained permission for access to classified information

In a context of fast developing electronic exchange of information and the impossibility of total control of information flow, cryptography is the only acceptable means for protection. At present it is one of the basic methods for ensuring confidentiality and integrity of information. Cryptographic security training is of great importance in the process of introducing cryptographic methods for classified information protection. According to Article 14 of CLASSIFIED INFORMATION PROTECTION ACT the Communication and Information Security Directorate (CISD) of the Ministry of Interior have the duty to provide the training of persons cleared for access to classified information in the use of cryptographic methods and devices. Regarding Article 14 and Article 65, Paragraph 1 and 2 of the REGULATION ON THE CRYPTOGRAPHIC SECURITY OF CLASSIFIED INFORMATION the CISD is only one authorized entity in Republic of Bulgaria that have a duties to organize and provide the training of cryptographic security administrators and users of cryptographic algorithms and devices.

CISD is the pioneer in cryptographic security training. It has a 25-seat auditorium but no computers to facilitate the handling of modern cryptographic means and the rules for their exploitation. Computer configurations would make the simulation of real time working conditions possible. Each working place will be defined as a cryptographic post and it will exchange encrypted information with the other posts. In this way the impartial assessment of the trained officers will be done by computer tests.

The necessary items are: 25 working positions with preferred configuration CPU Intel Pentium IV 3 GHz, 512 MB DDRRAM, 160 GB HDD, FDD, DVD RW, connected in a local network with LAN switch, laser color printer and flat scanner for preparing training materials. The abovementioned configurations need the following software: Windows XP, Office 2003.

The main purpose of this project is to harmonize the national criteria for protection of classified information with the EU Requirements: Agreement between the EU and the NATO on the security of information; Security Regulations of the Council of the EU - Basic Principles and Minimum Standards of Security Protection of Information Handled in Information Technology and Communication Systems; Council Decisions of the Commission of the European Communities and ISO/IEC 17799, BS 7799 Part 1 and Part 2, Common Criteria ISO 15408. The harmonization is a prerequisite for the international mutual recognition of the certificates which summarize the results of the IT evaluations and confirm that the evaluations have been done properly. For more details on the correspondence between the activities foreseen under this project and the EU Requirements see Annex 7, Table 1.

NOTES:
(*) – CISD – Communication and Information Security Directorate
(***)- Anechoic chamber – use for a variety of indoor antenna measurements, electromagnetic interference (EMI) measurements, electromagnetic compatibility (EMC) measurements, radiated emissions measurements of PCs and cryptographic devices included in AISs and networks, and TEMPEST equipment measurements.

The aforementioned classified information is in use at the following institutions of the Republic of Bulgaria:

1. Parliament
2. Council of Ministers (Government)
3. All ministries, include MoI
4. Regional and local self-government authorities
5. Court
7. Chief Prosecutor’s Office
8. Tax administration
9. Customs
10. Some trading corporations, etc.

Some institutions have several AIS.

3.2 Sectoral rationale
N/A

3.2.1 Identification of projects
N/A

3.2.2 Sequencing
N/A

3.3 Results
The successful project implementation will contribute to the effective implementation of the policy of the Republic of Bulgaria on classified information protection and the equipment modernisation for preventing unauthorised access to classified information in public administration.

3.3.1. Institution Building

3.3.1.1. Developed and implemented normative regulations and practice, corresponding to Agreement between the EU and the NATO on the security of information; Security Regulations the Council of the EU - Basic Principles and Minimum Standards of Security Protection of Information Handled in Information Technology and Communication Systems; Council Decisions of the Commission of the European Communities and ISO/IEC 17799, BS 7799 Part 1 and Part 2,
Common Criteria ISO 15408 standards and requirements for certification of personal computers, encrypting devices and AIS, used in work with classified information;

3.3.1.2. Training in improvement of the qualification of CISD(*) and SAA(**) – MoI officers, working on the problems of classified information protection on the basis of delivered modern equipment and the Agreement between the EU and the NATO on the security of information; Security Regulations the Council of the EU - Basic Principles and Minimum Standards of Security Protection of Information Handled in Information Technology and Communication Systems; Council Decisions of the Commission of the European Communities and ISO/IEC 17799, BS 7799 Part 1 and Part 2, Common Criteria ISO 15408 standards and requirements.

3.3.1.3. Overall improvement of the security of AIS and networks, working with classified information.

3.3.1.4. Organisational and administrational framework, necessary for the complete equipment of the laboratories and the auditorium for training MoI and public administration officers established.

3.3.2. Investment support

Technical, informational and other equipment for effective counteraction against all attempts at unauthorised access to AIS and networks for classified information transfer supplied;

3.4 Activities (including Means)

The above mentioned results will be achieved gradually through the implementation of the following activities:

3.4.1. Institution Building

3.4.1.1. Assistance in further development of the organisation and administration framework necessary for the classified information protection on the basis of Agreement between the EU and the NATO on the security of information; Security Regulations the Council of the EU - Basic Principles and Minimum Standards of Security Protection of Information Handled in Information Technology and Communication Systems; Council Decisions of the Commission of the European Communities and ISO/IEC 17799, BS 7799 Part 1 and Part 2, Common Criteria ISO 15408 standards and requirements;

3.4.1.2. Provision of a system for maintenance of adequate training and qualification of the CISD (*) and SAA(**) (MoI) officers, working on the problems of classified information protection;

3.4.1.3. Consultant assistance for development of procedures for initial assessment at the very beginning when the AIS or the network is still under design;

3.4.1.4. Assistance in elaboration of methods and standards for each of the measurement processes connected with the certification of PCs and cryptographic devices included in AIS and networks and measurement of the AIS and networks themselves;

3.4.2. Investment support

Supply of specialised equipment and software and measurement devices of the anechoic chamber(***), laboratory, the laboratory environment for testing the encrypting devices and their crypto-algorithms, creation of mobile laboratory for AIS certifying, and equipment of the auditorium.

3.5 Linked Activities:
The project is directly related to finalized or ongoing PHARE projects and will be based on the results achieved through them, as follows:

- **PHARE 1999 – BG 9911.02** – Institutional strengthening of the Bulgarian police: updating the criminal information system and improving management techniques;
- **PHARE 2000 – BG 0005.02** – Modernization of the equipment for border police control at the Bulgarian-Turkish border;
- **PHARE 2002 – BG 0203.10** – Implementation of the National Action Plan for the Adoption of the Schengen acquis: establishment of a national information system in accordance with Schengen requirements. Under the project, a system for criminal analysis of the operational situation, in accordance with Europol requirements, is being established;
- **PHARE 2002 – BG 0203.02** – Implementation of the National Strategy for Countering Corruption: development of a unified system for countering corruption at the Ministry of the Interior;
- **PHARE 2002 – BG 0203.03** – Creation of a unified system for evaluation, qualification and development of human resources;
- **PHARE 2003 Twinning light** – Supporting the Ministry of the Interior in strengthening the capacity of the Migration Directorate with the Ministry of the Interior for implementation of European norms
- **PHARE 2003 – BG 03/004-937.08.03** – Institutional building of the Academy of the Ministry of Interior and improving the quality of training;
- **PHARE 2004 - 2004/016-711.08.04** - Modernising Bulgarian police and enhancing its efficiency – supporting the Ministry of Interior in computerization and consolidation of the information and computing powers of the Ministry with the view to effectively exploiting police automated information systems in compliance with the EU standards. Under this project a Strategy for consolidation of the information and computing powers of the MoI and an Action Plan implementing the Strategy will be elaborated.

The project is connected with the proposed multi-year fiches on PHARE 2004 – 2006 in the sub-sector Police/Crime for protection of human rights, improving data exchange and strengthening a state authority for execution of the state policy in the field of migration; the sub-sector Borders for establishment and development of the information system for border control and countering illegal migration, as well as the sector Reform of State Administration for improvement of the public administrative services through electronic services in accordance with Bulgarian Laws:

- To set up a system for protection of the classified information, information technologies and information means.
- Adopted Classified Information Act and related regulations.
- Created the Rules on the Implementation of the Classified Information Protection.

Article 14 of CLASSIFIED INFORMATION PROTECTION ACT specify that the Communication and Information Security Directorate (CISD) of the Ministry of Interior have a duty to provide the training of persons cleared for access to classified information in the use of cryptographic methods and devices – security officers in all government institutions (President, Parliament, Council of Ministers (Government), All ministries, include MoI, MoD, MoFA, Regional and local self-government authorities, Court, National Investigation Service, Chief Prosecutor’s Office, Tax administration, Customs and trading corporations, etc). The Academy of the Ministry of Interior has a new module in its syllabus “Protection of the Classified Information” but according to Art. 14 and REGULATION ON THE CRYPTOGRAPHIC SECURITY OF CLASSIFIED INFORMATION the CISD is the only authorized entity in Republic of Bulgaria that have a duty to organize and provide the training of cryptographic security administrators and users of cryptographic algorithms and devices. This specialized training also requires special equipment that will be ensured for the functioning of the auditorium and is not available at the Academy of the MoI.
3.6 Lessons learned:
The Ministry of the Interior has gained valuable experience in the area of management and implementation of PHARE projects. This experience is based on the experience and results achieved through the implementation of previous projects BG 9911.02, BG 0005.02, BG 0012.02, BG 0203.01, BG 0203.10, as well as the implementation of a system for surveillance and self-assessment.

The projects developed under the program contribute to the strengthening of the institutional capacity of the Ministry of the Interior in line with the standards and achievements of the EU legislation in the area of Justice and Home Affairs.

The overall activity under the PHARE Program makes it possible for the Ministry of Interior structures to develop their capacity for planning, elaborating, management, implementation and monitoring of projects. It is an important precondition for solving key issues related to police management in accordance with the standards and legal norms of EU in the field of Justice and Home Affairs.

4. Institutional Framework
Beneficiary of the project will be the Ministry of Interior.
In the realization of the project will participate experts from different structural units of the Interior Ministry (Communication and Information Security Directorate, Communications Directorate, Operational and Technical Information Directorate, DKIAD, IST(Institute for Special Technique and others), but the overall management, realization and coordination of the activities will be done by the Communication and Information Security Directorate – MoI.
With the aim of securing an effective coordination and a good interaction between the directorates of MoI, that participate in the project, a Steering Committee will be created, that will be responsible for the following:

- approval of the decisions, taken during the time of the project activities;
- directing the activity of the separate working groups on the project;
- securing the full information that is necessary for the project;
- determining the persons for contact from each of the participating directories of the Ministry of the Interior;
- taking actions and measures in due time for the realization of the project in case of a delay;

The Steering Committee will include representatives of the Communication and Information Security Directorate, Communications Directorate, Operational and Technical Information Directorate, DKIAD and IST (Institute for Special Technique). The Committee will meet once in every 6 months, and when it is necessary even more often.
5. Detailed Budget

<table>
<thead>
<tr>
<th></th>
<th>Phare/Pre-Accession Instrument support</th>
<th>Co-financing</th>
<th>Total Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>€M 1,667</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Year 2005 - Investment support jointly co funded</th>
<th>National Public Funds (*)</th>
<th>Other Sources (**)</th>
<th>Total Co-financing of Project</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contract 2 - Supply</td>
<td>0.800</td>
<td>0.267</td>
<td>1.067</td>
</tr>
<tr>
<td>Investment support – sub-total</td>
<td>0.800</td>
<td>0.267</td>
<td>1.067</td>
</tr>
<tr>
<td>% of total public funds</td>
<td>max 75 %</td>
<td>min 25 %</td>
<td></td>
</tr>
</tbody>
</table>

In case of parallel co-funding (per exception to the normal rule, see special condition as indicated below:

<table>
<thead>
<tr>
<th>Year 2005 - Investment support co-funded in parallel</th>
<th>National Public Funds (*)</th>
<th>Other Sources (**)</th>
<th>Total Co-financing of Project</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Investment support – sub-total</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>% of total public funds</td>
<td>max 75 %</td>
<td>min 25 %</td>
<td></td>
</tr>
</tbody>
</table>

| Year 2005 Institution Building support              |                          |                    |                               |
| Contract 1 – Twinning                               | 0.600                    |                    | 0.600                         |
| IB support                                          | 0.600                    |                    | 0.600                         |
| Total project 2005                                  | 1.400                    | 0.267              | 1.667                         |

| Year 2006 Investment support                        | N/A                      |                    |                               |
| indicative Year 2006 Investment support             | N/A                      |                    |                               |
| indicative Year 2006 IB support                     |                          |                    |                               |
| Total (indicative) project 2006                     |                          |                    |                               |

(*) contributions form National, Regional, Local, Municipal authorities, FIs loans to public entities, funds from public enterprises

(**) private funds, FIs loans to private entities

National co-financing of up to 10% of the PHARE twinning support will be ensured by National Fund Directorate, Ministry of Finance. National co-financing will be ensured in the form of joint co-financing with PHARE funds.
6. Implementation Arrangements

6.1 Implementing Agency
The implementing agency for the project is Central Financing and Contracting Unit (CFCU) of the Ministry of Finance
102 “Rakovski” St.
tel.: +359298592772
fax: +359298592773.

CFCU will be responsible for organizing tenders, delivery of equipment and will carry out financial control during the time of the realization of the project.
The MoI will coordinate the production of the technical specifications, will nominate the respective experts for participation in the evaluation of the offers, will control the delivery, installing and configuring of the equipment.
The technical specifications for all investment components of the project will be worked out by the experts of the Communication and Information Security Directorate – MoI, together with the foreign experts, participating in the project.

6.2 Twinning
The IB component of the project is foreseen to be done by a 1,5 year standard twinning. For the purpose standard twinning procedures will be used.

In the framework of the twinning will be prepared the tender documentation for specialized equipment, necessary for fulfilling the aims of the project.

The realization of the project needs a Resident Twinning Advisor, who will be assisted by short-term experts from EU Member Countries.

The Resident Twinning Advisor has to be a civil servant of medium or high rank and has to have good communicative skills.

The Resident Twinning Advisor has to have a good knowledge in the following areas

- Knowledge and practical experience of EU best practices for:
  - encryption devices and crypto algorithms for them;
  - making and certifying of AIS and networks;
  - measuring of electromagnetic radiation and microwave measurements;
  - IT.

- Legal aspects (legal documents of the EU, and other conventions, decisions and acts of EU, connected with the protection of classified information).

The Twinning Resident Advisor has to be in a position to offer effective help in organizing the activities, connected with the project, specifying the characteristics of the technical means for delivery and in working out of the programs for training.
A very good knowledge of English, both written and spoken, is necessary.

Project Manager
Mr. Dipl. Eng. Chavdar Penkov
Director
Communication and Information Security Directorate – MoI
“6 September” Street №29
Tel.: +359 2 982 25 27
6.3 Non-standard aspects
The project will be managed by the rules of PHARE program and in accordance with the recommendations of the Twinning Manual and the PHARE Programming Guide

The Bulgarian side will insure the necessary for the realization of the project means from the national co-financing from the national budget through the National Fund Directorate – Ministry of Finance. The financial means from the national co-financing will be subject to reaching an agreement together with the means from the PHARE program.

6.4 Contracts
The expected according to the project contracts will be reached and realized according to the rules of the PHARE program. Expected number of contacts:

- Contract 1 – Twinning – 600 000 EUR
- Contract 2 – Supply – Contract for supply of technical, IT and other equipment – measuring apparatus and laboratory in the anechoic chamber, testing laboratory for encryption devices and the crypto algorithms in them, creating the mobile laboratory for certifying of the AIS and equipping the hall for training – 1 067 000 EUR

7. Implementation Schedule

7.1 Start of tendering/call for proposals
Selection a twinning partner – December 2005;
Start of twinning activity - 2006

7.2 Start of project activity- 2006

7.3 Project completion- 2007

8. Equal Opportunity
MoI guarantees equal opportunities for the participation of men and women in the implementation of the project.

9. Environment
This project will have no effect upon the environment.

10. Rates of return
For this project it is impossible to make an analysis for the rates of return. After its realization the project will have an operative effect in the area of the struggle against crime.
11. **Investment criteria** (applicable to all investments)

11.1 Catalytic effect
Adopting and applying EU rules and standards in the area of securing classified information is part of the overall process of the preparation of the Republic of Bulgaria for membership in the European Union.

Consultation aid and investments coming from PHARE program accelerate the processes of elaborating the national regulation, the organization and the technology of the work for taking measures against unauthorised access to classified information, the strengthening of the capacity for the use of centralized AIS and the enhancement of the effectiveness of the work for the prevention of criminal activity in this area.

11.2 Co-financing
The Bulgarian authorities will secure from the national budget at least 25% national co-financing of the investment part of the project and up to 10% of the value of the twinning component.

11.3 Additionality
This project does not have financial reimbursement, that will attract sources for financing from the private sector or from the international financial institutions. The financial help of the PHARE program will not duplicate sources from the republican budget or from other bilateral aid.

11.4 Project readiness and size
During the work upon the problems and tasks, connected with the fulfillment of the priorities of the Bulgarian police a research was made upon the needs and the possibilities. The necessary preliminary technical research, that is shown in Annex 4, was also made.
The investments on the project cover the requirements for the minimal amount. The financial support of PHARE will be 1 400 000 EUR.

11.5 Sustainability
The investments in the project are in accordance with the norms and standards of the EU. The realization of the project will have no effect upon the environment.

11.6 Compliance with state aids provisions
N.A.

12. **Conditionality and sequencing**
The Bulgarian authorities will continue to show their commitment to accept and apply *acquis* and the practical standards of the EU for preventing unauthorised access to classified information.

Before the beginning of the actual realization of the project the tasks and the responsibilities of each of the participating structures of the MoI will be determined and approved. In this respect there is a great deal of experience that is acquired. At this stage the concerned structures have exchanged preliminary information about the realization of the project and the allocation of the tasks and duties.
The project, accomplished by twinning, requires the full involvement and participation of the leadership of the beneficiary of the project. That is why the leadership of the ministry promises to secure to its twinning partner the sufficient and well prepared staff and support (including translation) and also to make institutional changes, which will be pointed out as necessary for the successful realization of the project. The necessary conditions for executing control of the realization of the project by the European commission and for taking in mind its prescriptions for correcting the mistakes will be secured.
During the work on the project the access of the twinning-partners and of the Bulgarian experts to all the necessary leadership levels will be guaranteed.

In case of unexpected delay in the realization of the project or some other impediments, the leadership of MoI, together with the twinning partner, will determine and take the necessary measures for overcoming them.

**ANNEXES TO PROJECT FICHE**

1. Logframe in standard format (compulsory) for each project - *see Annex 6 of this Guide for guidance* – plus (optional) sector monitoring sheet for sector programmes

2. Detailed implementation chart (compulsory for year 1, optional for future years)

3. Contracting and disbursement schedule, by quarter, for full duration of project (including disbursement period) (compulsory for year 1)

4. For all projects: reference list of feasibility/pre-feasibility studies, indepth ex ante evaluations or other forms of preparatory work. For all investment projects, the executive summaries of economic and financial appraisals, environmental impact assessments, etc, should be attached (compulsory)

5. Reference list of relevant laws and regulations (compulsory)

6. Reference list of relevant strategic plans and studies (may include institution sector strategies, development plans, business development plans, etc) (compulsory)

   1. Logframe in standard format;
   2. Detailed implementation chart;
   3. Contracting and disbursement schedule, by quarter, for full duration of project (including disbursement period);
   4. Reference list of feasibility/pre-feasibility studies on the basis of assessment of necessary equipment;
   5. Reference list of relevant laws and regulations;
   6. Reference list of relevant strategic plans and studies.
   7. Table 1 – Correspondence between activities and EU Regulations
   8. Table 2 – Existing and Necessary equipment
## LOGFRAME PLANNING MATRIX FOR

**Further Strengthening of the Administrative Capacity of Bulgarian Police and Providing Conditions for Application of the Classified Information Protection Law in the Public Administration of the Republic of Bulgaria – a Stage in the Protection of EU Classified Information.**

<table>
<thead>
<tr>
<th>Programme name and number:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BG 2005/017-586.02.01</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contracting period expires:</th>
<th>End of execution of contracts expires:</th>
</tr>
</thead>
<tbody>
<tr>
<td>30 November 2007</td>
<td>30 November 2008</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Total budget:</th>
<th>Phare budget:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 667 000 EUR</td>
<td>1 400 000 EUR</td>
</tr>
</tbody>
</table>

### Overall objectives

- To further strengthen the security unit in the Ministry of Interior responsible for the implementation of the classified information protection policy of the Republic of Bulgaria and modernize procedures (SOPs – standard operating procedures), organisation and management systems, and equipment to authorise and monitor access to classified information and prevention of unauthorized access to it in line with Agreement between the EU and the NATO on the security of information; Security Regulations the Council of the EU - Basic Principles and Minimum Standards of Security Protection of Information Handled in Information Technology and Communication Systems; Council Decisions of the Commission of the European Communities and ISO/IEC 17799, BS 7799 Part 1 and Part 2, Common Criteria ISO 15408.

### Objectively Verifiable Indicators

- Achieving conformity with the Accession Partnership and NPAA priorities
- Putting in place SOPs, management & organisation practices to allow and monitor access to classified information
- Transparent rules for the classification levels and procedures of information
- Elaboration of a normative regulation needed to secure logical, cryptographic and administrative protection of classified information, AIS and networks
- Reduction of unauthorized access level;
- Number of officers trained in classified information protection against unauthorized access increased;
- Supply of specialised equipment needed to test and certify public administration AISs and networks existing or under construction.

### Sources of Verification

- European Commission Regular Report;
- Phare Reports;
- Annual report on National Schengen Action Plan implementation;
- Official statistics about the level of crime;
- Other official documents, analyses and reports, worked out by the European Commission and Bulgarian authorities.

### Project purpose

- To achieve a higher effectiveness of police activities by adoption and implementation of the best practices in prevention and protection of Automated Information Systems (AIS) and public

### Objectively Verifiable Indicators

- Complete organisation rethinking, introduction of administrative procedures and monitoring, and introduction of equipment and modernization of the existing

### Sources of Verification

- Reports of the Pre-accession progress Councillor;
- Report of the Project Supervision Committee;

### Assumptions

- Mol demonstrates capacity for counteraction to crime, in accordance with EU requirements and standards;
- Implementation of the
<table>
<thead>
<tr>
<th>Laboratory and auditorium of CISD(^{(1)}) Ministry of Interior (MoI).</th>
<th>• Enhancement of the qualification of CISD(^{(1)}) and SAA(^{(1)}) officers, working under the Classified Information Protection Law (CIPL), on the basis of training courses for exploitation of new equipment and introduction of Agreement between the EU and the NATO on the security of information; Security Regulations the Council of the EU - Basic Principles and Minimum Standards of Security Protection of Information Handled in Information Technology and Communication Systems; Council Decisions of the Commission of the European Communities and ISO/IEC 17799, BS 7799 Part 1 and Part 2, Common Criteria ISO 15408 standards and requirements.</th>
<th>• Reports for participation of EU representatives in the training, carried out in MoI Academy; • MoI Reports; • Reports on the MoI structures activities; • - Statistical data about accomplished activities.</th>
<th>National Strategy for Counteraction to Crime 2002-2005, in its section on reforms in security and public order services.</th>
</tr>
</thead>
</table>

\(^{(1)}\) CISD - Criminal Investigation Service of the Interior, SAA - Special Anti-terrorist Service of the Interior.
## Results

### Institutional building

- Developed and implemented normative regulations and practice, corresponding to Agreement between the EU and the NATO on the security of information; Security Regulations the Council of the EU - Basic Principles and Minimum Standards of Security Protection of Information Handled in Information Technology and Communication Systems; Council Decisions of the Commission of the European Communities and ISO/IEC 17799, BS 7799 Part 1 and Part 2, Common Criteria ISO 15408 standards and requirements for certification of personal computers, encrypting devices and AIS, used in work with classified information;
- Training in improvement of the qualification of CISD\(^\text{(*)}\) and SAA\(^{(**)}\) – MoI officers, working on the problems of classified information protection on the basis of delivered modern equipment and the Agreement between the EU and the NATO on the security of information; Security Regulations the Council of the EU - Basic Principles and Minimum Standards of Security Protection of Information Handled in Information Technology and Communication Systems; Council Decisions of the Commission of the European Communities and ISO/IEC 17799, BS 7799 Part 1 and Part 2, Common Criteria ISO 15408 standards and requirements
- Overall improvement of the security of AIS and networks, working with classified information.
- Organisational and administrational framework, necessary for the complete equipment of the laboratories and the auditorium for training MoI and public administration officers established

### Objectively Verifiable Indicators

- A completed normative regulation for security and protection of the informational and communications systems by the end of the project implementation by 3 Q 2007;
- Completed courses for enhancing the qualification of the employees of the Communication and Information Security Directorate – MoI, working on the application of the Classified Information Protection Law – for work with new equipment and introduction to the new European norms and standards in the area of protection and prevention of informational an communications systems:
  - Training of min 3 trainers in working with encrypting devices and methods for officers with authorised access to classified information;
  - Training of min 4 trainers in coordination and control of the protection against spurious electromagnetic emissions from technical devices processing, storing and transmitting classified information involves tests for electromagnetic emissions in an anechoic chamber;
  - Training of min 6 trainers in process of issuing security certificates of AIS or networks working with classified information includes accreditation of these AIS or networks.
- Fully equipped and modernized laboratories needed to certify computers, AISs and networks of the MoI and the public administration using classified information and a

### Sources of Verification

- Monitoring by the Delegation of the European Commission (EC);
- PAA and technical assistance reports;
- Technical assistance reports;
- Protocols of conducted technical expertise and measurements;
- Protocols of accomplished installation and testing of technical devices;
- Protocols of approved stages of the system introduction;
- Officers training schedules;
- Protocols of conducted officers training;
- Tender documentation;
- Statistical data about MoI investigation activities.

### Assumptions

- Adopted and implemented Personal Data Protection Law and the related bylaws;
- Adopted and implemented Classified Information Protection Law and the related bylaws;
- Adequate support of the activities by the national budget.
### Investment support

- Technical, informational and other equipment for effective counteraction against all attempts at unauthorised access to AIS and networks for classified information transfer supplied.

  - a testing laboratory for simulation of actual working conditions of a large variety of cryptographic communication devices and for certifying cryptographic devices and algorithms for them
  - a mobile laboratory for analysis, monitoring and certification of AISs and networks
  - the purchase of a high precision system with specialized software needed to certify of PCs and cryptographic devices included in AISs and networks
  - a hall for training of experts to be trained in working with cryptographic devices located at the premises of the whole public administration;
  - workshops, seminars and training in application of EU legislation and regulations in the field of collecting, storing, processing, transmitting and utilising data and inter-institutional co-operation at national and international level;
  - workshops, seminars and training in new devices, technical and normative acts;
  - Certify trainers in Certified Education Centers – national and EU
<table>
<thead>
<tr>
<th>Activities</th>
<th>Means</th>
<th>Assumptions</th>
</tr>
</thead>
</table>
| **Institutional Building**                     | • Assistance in further development of the organisation and administration framework necessary for the classified information protection on the basis of Agreement between the EU and the NATO on the security of information; Security Regulations the Council of the EU - Basic Principles and Minimum Standards of Security Protection of Information Handled in Information Technology and Communication Systems; Council Decisions of the Commission of the European Communities and ISO/IEC 17799, BS 7799 Part 1 and Part 2, Common Criteria ISO 15408 standards and requirements  
  • Assistance in elaboration of methods and standards for each of the measurement processes connected with the certification of PCs and cryptographic devices included in AISs and networks and measurement of the AISs and networks themselves;  
  • Consultant assistance for development of procedures for initial assessment at the very beginning when the AIS or the network is still under design  
  • Provision of a system for maintenance of adequate training and qualification of the CISD(*) and SAA(**) (MoI) officers, working on the problems of classified information protection.  
  • Supply of specialised equipment and software and measurement devices of the anechoic chamber(***) laboratory, the laboratory environment for testing the encrypting devices and their cryptographical algorithms, creation of mobile laboratory for AIS certifying, and equipment of the auditorium. | • A Twinning agreement for TRA and short-term experts for the project duration.  
  • Implementation of the Twinning covenant;  
  • A Contract for supply of the equipment needed;  
  • Submission of Technical specifications;  
  • Training on new equipment delivered. | • Number of officers trained in operating with the information systems increased;  
  • Minutes of expert meetings for validating the stages of the system set up;  
  • Tender documentation;  
  • Minutes of training provided for the MoI officials;  
  • Minutes of completed installation and test of the technical equipment;  
  • Statistics on MoI activities;  
  • Schedules of officers’ training. |
| **Investment Support**                         |                                                                       | • Involvement of the leadership and executive personnel of all MoI structures, connected with the project implementation, and also of consultants from the Council of Ministers and the Ministry of Justice of the Republic of Bulgaria;  
  • Involvement of the Executive agency during tender and contracting procedures;  
  • Adequate training of the executive personnel in systems exploitation. |
Notes:
The Ministry of Interior Act (MoIL) – article 124, paragraph 1, point 1 and 2, and the Classified Information Protection Act (CIPA) – article 14, envisage the following major priorities in the work of the Communications and Information Security Directorate:

5. Cryptographic protection of classified information (National Communication/Cryptographic Security Authority (NCSA) and National Distribution Authority (NDA));
6. Issuance of security certificates of AIS or networks working with classified information (Security Accreditation Authority (SAA));
7. Coordination and control of the protection against spurious electromagnetic emissions from technical devices processing, storing and transmitting classified information;
8. Implementation and supervision of training courses in application of cryptographic methods and means by officers who have obtained permission for access to classified information.

(*) - CISD – Communications and Information Security Directorate
(***) - Anechoic chamber – use for a variety of indoor antenna measurements, electromagnetic interference (EMI) measurements, electromagnetic compatibility (EMC) measurements, radiated emissions measurements of PCs and cryptographic devices included in AISs and networks, and TEMPEST equipment measurements.
## DETAILED IMPLEMENTATION CHART

<table>
<thead>
<tr>
<th>Component</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>D</td>
<td>J</td>
<td>F</td>
</tr>
<tr>
<td></td>
<td>M</td>
<td>A</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td>J</td>
<td>A</td>
<td>S</td>
</tr>
<tr>
<td></td>
<td>O</td>
<td>N</td>
<td>D</td>
</tr>
<tr>
<td></td>
<td>J</td>
<td>F</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td>A</td>
<td>M</td>
<td>J</td>
</tr>
<tr>
<td></td>
<td>J</td>
<td>A</td>
<td>S</td>
</tr>
<tr>
<td></td>
<td>O</td>
<td>N</td>
<td>D</td>
</tr>
</tbody>
</table>

### Contract 1 - Twinning

| Quarter | C | I | I | I | I | I | I | I | I | I | I | I |

### Contract 2 - Supply

| Quarter | T | T | T | C | I | I | I |

C – contracting; I - implementation.

### CONTRACTING AND DISBURSEMENT SCHEDULE (by quarter, for full duration of the project)

#### Components 2006 2007 2008 2009 2010

<table>
<thead>
<tr>
<th>Components</th>
<th>1 quart.</th>
<th>2 quart.</th>
<th>3 quart.</th>
<th>4 quart.</th>
<th>1 quart.</th>
<th>2 quart.</th>
<th>3 quart.</th>
<th>4 quart.</th>
<th>1 quart.</th>
<th>2 quart.</th>
<th>3 quart.</th>
<th>4 quart.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contract 1 – Twinning</td>
<td>0,600</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contracting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disbursement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Components</th>
<th>1 quart.</th>
<th>2 quart.</th>
<th>3 quart.</th>
<th>4 quart.</th>
<th>1 quart.</th>
<th>2 quart.</th>
<th>3 quart.</th>
<th>4 quart.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contract 2 – Supply</td>
<td>1,067</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contracting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disbursement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1,067</td>
</tr>
</tbody>
</table>

All figures are in million Euros
Reference to pre-feasibility studies on the basis of assessment of necessary equipment

The main objectives and purposes of the project are defined by the necessity of strengthening MoI capacity for realization of the activities, connected with classified information protection. The preliminary analyses of the possibilities for solving this problem require improvement of the technical resources and enhancement of the quality of qualification of CISD-MoI officers, that work on the problems.

The first of the analyses is based on the development of the computing resources and the public administration computerizing, which leads to increasing number of modernized, developing and future AIS, processing classified information. All these, including the already existing ones, must meet the requirements of the Classified Information Protection Act (CIPA) and the relevant normative acts, and except the certification at adoption level, they are subject to regular pre-certification. Along with the rapid development of information technologies, this extends the volume of the classified information protection activities.

The second analysis is directed towards assessment of possibilities for improvement of the effectiveness through optimisation of exploitation and modernisation (by additional equipment and/or replacement of out-of-date modules) of already existing facilities, and enhancement of personnel qualification.

On the third place, the specialised equipment market for measurement and analysis is explored. This equipment is applicable to the following activities:

- verification of all encrypting devices and of the crypto-algorithms, used in them;
- accreditation of AIS and networks for classified information processing;
- measurement of spurious electromagnetic emissions of the technical devices.

Computer configurations, software support and computer peripheral devices are also examined for the purposes of training in work with cryptographic methods and means of officers with authorised access to classified information.

The analyses were made during the Project Fiche preparation and their approximate financial assessment is considered in the presented budget.

In view of the objectives and the purposes of the government Management Programme, and in view of the recommendations of EU Regular reports on Bulgaria’s progress, the implementation of this project will contribute to the enhancement of effectiveness in the combat against crime, to improvement of the quality of police investigation and the human rights respect in compliance with EU requirements in the field of justice and home affairs.

The rapid development of electronic exchange and lack of possibility for total control of the information flows established cryptography as the optimal decision for securing the confidentiality and wholeness of the information. With the purpose of training officers with authorised access to classified information in work with cryptographic methods and means, a training room with 25 seats was built in CISD, but there is no computer equipment, that will illustrate and facilitate the assimilation of the modern cryptographic means and the principles of work with them. The supply of such equipment will give opportunity for simulation of real work conditions and will create conditions for objective assessment of the trained officers.
For verification of encrypting devices and the crypto-algorithms, used in them, in CISD started construction of testing laboratory for simulation of the real working environment of a large scale encrypting communicational devices. Bearing in mind the big variety of these devices and the fast development of the technologies in the field, it is important that the technical and software support of the laboratory environment maintain broad scope of network protocols and transmission media in order to improve the effectiveness and speed of work. For verification of the new and repaired devices sample encrypting device is necessary, with which at the present the laboratory is not equipped. Because of lack of separated modules for the available devices (hardware protocol analyser), a part of the new equipment cannot be verified.

A serious problem is caused also by the real-time operation of the same equipment, especially in data analysis and processing, transferred on the basis of high-speed standards of GigaBit Ethernet, STM-1e/EC-3 or STM-4/OC-12 type.

For the solution of these and other problems in the technical improvement of the laboratory environment for equipment testing, the purchase of a new hardware protocol analyser is necessary and active communicative devices (concentrators, routers and others) for development of transmission medium.

With the purpose of qualification, in view of the electromagnetic emissions, of the technical means, including those used in the MoI services, an anechoic chamber, type RFD-F/A-100, is built and equipped and the construction of laboratory for electromagnetic measurements has started. The laboratory has also at its disposal calibrated antennas in the range from 100 Hz to 18 GHz. The available installations are not specialised in electromagnetic interferences measurement and their model is 10 years old with relatively weak sensitiveness (max –115 dBm). For comparison, today are offered specialised spectrum analysers with sensitiveness –150 dBm. For the measurements accuracy to be guaranteed, it is necessary that cables, amplifiers and antennas are periodically measured for VSWR, amplification and losses, and on that basis the algorithms, used in the calculations of the final results, to be corrected. At the moment the laboratory doesn’t have the necessary microwave vector analyser.

The enlargement of the computing resources and the computerisation of the public administration have led to increased use of AIS and networks for classified information processing. Along with the rapid development of information technologies and the amendments in the regulations on classified information protection, this imposes the necessity of scrutinized analysis of the AIS and networks and check-ups for spurious electromagnetic emissions in the process of accreditation of the developing and already existing systems. In view of the large variety of the used technical equipment and software support in the networks, the audit of the networks and AIS is possible only with the assistance of specialised measurement equipment and software (networks and protocols analysers, products for security analysis and others), that maintains wide range of network protocols and transmission media. At the present CISD does not have at its disposal such equipment, software and suitable vehicle for transportation of the accreditation team and the relevant equipment.

The CISD-MoI officers, who work on the problems of classified information protection, have high qualification, but bearing in mind the dynamics in the spheres of technology and the related regulations, there is necessity of training courses for operation with the specialized facilities, used in specific measurements and analyses, and also of courses for introduction to EU standards in this field, with respect to their enforcement in practice.
Reference list of relevant laws and regulations

- Ministry of Interior Act (MoIA);
- Classified Information Protection Act (CIPA);
- Law on the Access to Personal Data (LAPD);
- Regulation on the Implementation of MoIL;
- Regulations on the Implementation of CIPL;
- Regulations on the Implementation of LAPD.

Detailed list of this regulations

I. MINISTRY OF INTERIOR ACT

Article 124.
Communication and Information Security Directorate (CISD) is a specialised unit of MoI for cryptographic protection of the classified information in the Republic of Bulgaria and in its diplomatic and consular representations, for acquiring, systematising and processing of information from foreign sources to the interest of the state security and operative control over the radio frequency spectrum by:

1. assessing and working out cryptographic algorithms and devices for cryptographic protection of the classified information; working out and distributing the used cryptographic keys; permitting and controlling the using, the production and the import of devices for cryptographic protection;
2. issuance of certificate for security of the automated informational systems or networks used for work with classified information; co-ordination and control of the activity on the protection of the technical devices against parasitic electromagnetic emissions of the technical devices processing, storing and transferring classified information;
3. organise and provide the communications of the Republic of Bulgaria with its diplomatic and consular representations and the cryptographic protection of the exchanged information providing the necessary personnel in the administrative units and in the diplomatic and consular representations;
4. acquire, process and systematise information by technical devices from technical sources of other countries to the interest of the national security and submit it to users determined by an order of the Minister of the Interior and by a law;
5. detect and prevent the use of the national radio frequency spectrum against the security of the country or in violation of the laws and interact with the competent state bodies;
6. provide and apply special reconnaissance devices and prepare material evidence under conditions and by an order determined by a law;
7. carry out operative and investigation activity;
8. interact with the other offices of MI and with the specialised state bodies, as well as with related offices of other countries, within the circle of their competence;
9. carry out informational activity.
II. CLASSIFIED INFORMATION PROTECTION ACT (Official Gazette No. 45/30.04.2002)

GENERAL PROVISIONS

Article 1
(1) This Act governs the public relations arising in connection with the generation, the processing, and the storing of classified information, and lays down the conditions and procedure for the release thereof and the access thereto.
(2) The purpose of this Act is to protect classified information from unauthorised access.
(3) Within the meaning of this Act, "classified information" is any information which is a State secret or an official secret, and any foreign classified information.

Article 2
This Act shall apply as well to any foreign classified information which may be made available by another State or an international organisation, insofar as an existing international treaty, to which the Republic of Bulgaria is a party, does not provide otherwise.

Article 3
(1) Access to classified information shall not be allowed to any person other than those having an appropriate clearance in keeping with the "need-to-know" principle, unless otherwise provided hereunder.

Classified Information

Article 25
State secret is such information, as listed in Schedule 1, the unauthorised access to which might threaten or prejudice such interests of the Republic of Bulgaria as relate to national security, defence, foreign policy or the protection of the constitutional order.

Article 26
(1) Official secret is such information as is generated or stored by government authorities or by the authorities of local self-government, is not a State secret, and the unauthorised access to which might adversely affect the interests of the State or prejudice another interest protected by law.
(2) The information which shall be the subject of classification as an official secret shall be determined by law.
(3) The heads of organisational units shall, within the limits hereunder, announce a list of the classes of information under paragraph 2 within their respective field of activity. The procedure for, and the manner of, such announcement shall be laid down in the Detailed Rules for the Application hereof.

Article 27
Foreign classified information is such classified information as has been disclosed by another State or by an international organisation in pursuance of an international treaty to which the Republic of Bulgaria is a party.

CLASSIFIED INFORMATION PROTECTION AUTHORITIES

Functions of the Security Services

Article 14
The Communication and Information Security Directorate (CISD) of the Ministry of Interior shall have a duty to:
1. perform the activities relating to the cryptographic protection of classified information in pursuance of Article 124 of the Ministry of Interior Act;
2. issue security compliance certificates of automated information systems (AIS) or networks used for operation with classified information;
3. coordinate and control the electromagnetic interference countermeasures protecting the technical devices used to process, store or transmit classified information;
4. provide and control the training of persons cleared for access to classified information in the use of cryptographic methods and devices.

Cryptographic Security

Article 87

(1) The generation and distribution of the necessary cryptographic keys shall be the responsibility of the CISO of the Ministry of Home Affairs. (NDA National Distribution Authority)

III. REGULATION ON THE GENERAL BINDING TERMS FOR SECURITY OF AUTOMATED INFORMATION SYSTEMS OR NETWORKS USED FOR CREATION, PROCESSING, STORAGE AND TRANSFER OF CLASSIFIED INFORMATION (Official Gazette No. 46/20.05.2003)

Security accreditation authority for AIS or networks

Article 3.

(1) The Security Accreditation Authority for AIS or networks (SAA), within the meaning of this Regulation, shall be the CISO of the Ministry of Interior.
(2) The security accreditation authority shall:
1. Issue recommendations and instructions on the security of AIS or networks;
2. Recommend a set of standards and devices, which can be used in AIS or networks for protection of classified information;
3. Approve the security documents of AIS or networks;
4. Make an overall security assessment of AIS or networks;
5. Issue security certificates of AIS or networks;
6. Lay down the terms for additional accreditation of AIS or networks;
7. Coordinate and control the activities for protection of technical devices used for processing, storage and transfer of classified information against parasitic electromagnetic radiation;
8. Keep a record of the certified AIS or networks.

IV. REGULATION ON THE CRYPTOGRAPHIC SECURITY OF CLASSIFIED INFORMATION (Official Gazette No. 102/21.11.2003)

Cryptographic (communication) security authority of the Republic of Bulgaria (NCSA)

Article 3.

The cryptographic (communication) security authority (NCSA) of the Republic of Bulgaria, for the purpose of this Regulation, shall be the CISO of the Ministry of Interior.

Article 4.

The NSCA of the Republic of Bulgaria shall:
1. implement the national policy for cryptographic protection of classified information, in accordance with the Classified Information Protection Act (CIPA), this Regulation and all bylaws on the protection of classified information;
2. issue directives and recommendations on all aspects of cryptographic security;
3. evaluate and approve cryptographic methods and means for protection of classified information;
4. participate in the overall security evaluation of cryptographic networks and in the approval procedure for their exploitation;
5. produce and distribute cryptographic keys for protection of classified information in the cryptographic networks of the Republic of Bulgaria;
6. participate in the overall security evaluation of systems for automated generation and distribution of cryptographic keys and in the approval procedure for their exploitation;
7. coordinate and control the application, production and import of means for cryptographic protection of classified information;
8. conduct training in cryptographic security and issue permissions for application of cryptographic means;
9. conduct consultations on the activities of cryptographic security officers;
10. permit and control the cryptographic security training conducted by other organizational units;
11. draw up statements in cases of cryptographic security compromise;
12. keep a record of the approved cryptographic means and networks.

**Plans and Conceptions**

- Conception about the Information Activities of MoI;

**Instructions**

- Ordinance of the General Requirements for Industrial Security;
- Ordinance of the System of Measures, Methods and Means for the Physical Security of Classified Information and the Terms and Procedure of Their Application;
- Ordinance of the Compulsory General Requirements for the Security of AIS and Networks, in which Classified Information is Created, Processed, Stored and Transferred;
- Ordinance of the Cryptographic Security of Classified Information.

**MoI Methods and Standards**

- Methods for verification of the cryptographic protection of information in encrypting devices designed and produced in the Republic of Bulgaria for the needs of national security and defence;
- Standards of protection of technical devices against spurious emissions.

ANNEX 6

**Reference list of relevant government strategic plans and studies**

- Governance Programme of the Bulgarian government;
- National Programme for the Adoption of the Acquis;
- Multi-annual Phare Programming Document;
- Updated National Strategy for Counteraction to Crime.
The purpose of CISD is harmonized national criteria for protection of classified information with EU criteria was that such harmonization is one of the prerequisites of international mutual recognition of the certificates which summarize the results of Information Technology (IT) security evaluations and confirm that the evaluations have been properly carried out. It is also a prerequisite of mutual recognition that the methods used to apply these harmonized criteria should themselves be harmonized.

<table>
<thead>
<tr>
<th>Objectives</th>
<th>Responsibilities and activities for the Communication and Information Security Directorate - MoI (CISD) for the implementation of the classified information protection policy of the Republic of Bulgaria (justifications)</th>
<th>Relevant EU standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accession Partnership (AP) priorities,</td>
<td>• The Ministry of Interior Act (MoIA) – article 124, paragraph 1, point 1 and 2,</td>
<td>• Agreement between the EU and the NATO on the security of information;</td>
</tr>
<tr>
<td>Catalogue of Main Administrative Structures for the Implementation of the Acquis, Road Map for Bulgaria, National Program for the Adoption of the Acquis (NPAA), Updated National Strategy for Combating Crime, Multi-annual Phare Programming Document</td>
<td>• The Classified Information Protection Act (CIPA)</td>
<td>• Security Regulations of the Council of the EU Basic Principles and Minimum Standards of Security Protection of Information Handled in Information Technology and Communication Systems;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Council Decisions of the Commission of the European Communities</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information technology - Code of practice for information security management</td>
</tr>
<tr>
<td></td>
<td>• ISO/IEC 17799,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• BS 7799 Part 1 and Part 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security functional requirements; Security assurance requirements; Evaluation methodology</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Common Criteria ISO 15408.</td>
<td></td>
</tr>
</tbody>
</table>

**Activities**
- Elaboration of basic rules for exploitation of communication and information systems in compliance with EU standards and requirements
- Development of a system for protection of classified information and information technologies, carriers and means;
- Protection of personal data and classified information against criminal acts.
- Public Administration Modernisation Strategy

- With accordance in this Acts CISD is Security Accreditation Authority (SAA), National Communication Security Authority (NCSA), National Cryptographic Authority (NCA), National Distribution Authority (NDA) for national classified information;

Functions:
Security organizations – National Security Authority:
1. A national organization responsible for the gathering of information on subversive activities and threat assessment;
2. an INFOSEC authority in charge of the analysis and reaction to technical threats;
3. a regular collaboration in the security domain
4. and the adoption of common standards.

Security of classified information – activities and definitions:
- Establishing a functional chain for the Security of Information Systems
- Communication and Information System (CIS)
- Security of a Communication and Information System (SCIS):
  - Accreditation – relevant documentation:
    ✓ System-specific Security Requirement Statement (SSRS)
    ✓ STRUCTURE and CONTENT OF SECURITY OPERATING PROCEDURES (SecOPs)
    ✓ SECURITY RISK ASSESSMENT AND RISK MANAGEMENT OF SECURE SYSTEMS
    ✓ MINIMUM REQUIREMENTS FOR THE ACCREDITATION OF MEMBER STATES INFOSEC ORGANISATIONS AS APPROPRIATELY QUALIFIED AUTHORITIES (AQUAS) FOR CONDUCTING SECOND PARTY EVALUATIONS OF
17. Conducts training of security officers for AIS or networks;
18. Keeps a record of certified AIS or networks.

• Cryptographic protection of classified information:
14. Implements the national policy on cryptographic security of classified information according to CIPA, this Regulation and other bylaws on classified information protection;
15. Provides guidance and recommendations on all cryptographic security aspects;
16. Evaluates and approves cryptographic methods and means for classified information protection;
17. Participates in the overall evaluation of the security of cryptographic networks and the approval of their exploitation;
18. Generates and distributes cryptographic keys for the protection of classified information in the cryptographic networks of the Republic of Bulgaria;
19. Participates in the overall evaluation of the security of systems for automated generation and distribution of keys and in the approval of their exploitation;
20. Coordinates and controls the exploitation, production and import of means for cryptographic protection of classified information;
21. Conducts training in cryptographic...
security and issues permissions for exploitation of cryptographic means;
22. Provides methodological instruction to cryptographic security officers;
23. Approves and controls cryptographic security training conducted by other organizational units;
24. Draws written statements in cases of cryptographic security compromise;
25. Keeps a record of approved cryptographic means and issues passports to all individually tested cryptographic means;

- Coordination and control of the protection against spurious electromagnetic emissions from technical devices processing, storing and transmitting classified information;
- Implementation and supervision of training courses in application of cryptographic methods and means by officers who have obtained permission for access to classified information.
- Conducts training of security officers for AIS on networks.

Definitions:
Accreditation means the authorisation and approval granted to a system to process European Union classified information in its operational environment.
Evaluation means the detailed examination, by an appropriate authority, of the security aspects of a system or of a cryptographic or a computer security product.
There are two kinds of evaluation: technical
evaluation and operational evaluation.

INFOSEC means the application of security measures to protect information processed, stored or transmitted in communication, information and other electronic systems against loss of confidentiality, integrity or availability, whether accidental or intentional, and to prevent loss of integrity and availability of the systems themselves. INFOSEC measures include those of computer, transmission, emission and cryptographic security, and the detection, documentation and countering of threats to information and to the systems.

A computer security product means a general item of computer security intended to be included in a system in order to improve or ensure the confidentiality, integrity or availability of the data processed.

Computer security, or COMPUSEC, means the installation on a computer system of security devices, programmed in hardware or in software, aimed at protecting against or preventing unauthorised disclosure, manipulation, modification or deletion of information or denial of access.

Communication security, or COMSEC, means the application to telecommunications of security measures intended to prevent unauthorised persons from accessing useful information by acquiring or examining the messages transmitted, or to ensure the authenticity of such messages.

TEMPEST protection means the application of measures intended to protect all or part of a system against threats resulting from compromising spurious emissions.

- Cryptographic protection of classified information includes testing of cryptographic devices and their cryptographic algorithms;
- The process of issuing security certificates on AIS or networks working with classified information includes accreditation of these AIS or networks;
• The coordination and control of the protection against spurious electromagnetic emissions from technical devices processing, storing and transmitting classified information involves tests for electromagnetic emissions in an anechoic chamber.
• Training in exploitation of cryptographic methods and means of officers who have obtained permission for access to classified information;
### TABLE 2 NECESSARY EQUIPMENT

#### ANNEX 8

<table>
<thead>
<tr>
<th>Justification</th>
<th>Available testing equipment</th>
<th>Necessary testing equipment</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Evaluates and approves cryptographic methods and means for classified information protection;</td>
<td>• Network Protocol Analyzer – J2300E Agilent Advisor Mainframe, based on 400 MHz processor and 256 MB RAM</td>
<td>• Powerful Protocol Analyzer for the other standards of the OSI model of communication protocols</td>
</tr>
<tr>
<td>• Participates in the overall evaluation of the security of cryptographic networks and the approval of their exploitation;</td>
<td>• The mainframe is equipped with following modules:</td>
<td>• Mainframe with significant improvement in performance and real time capture and analysis.</td>
</tr>
<tr>
<td>• Generates and distributes cryptographic keys for the protection of classified information in the cryptographic networks of the Republic of Bulgaria;</td>
<td>• J3444 A – LAN Fast Ethernet under cradle</td>
<td>• The mainframe to be equipped with modules for analysis of:</td>
</tr>
<tr>
<td>• Coordinates and controls the exploitation, production and import of means for cryptographic protection of classified information;</td>
<td>• J2296 D – E1 BNC 75 Ohm interface module</td>
<td>⇒ LAN Gigabit Ethernet</td>
</tr>
<tr>
<td>• Draws written statements in cases of cryptographic security compromise;</td>
<td>• J4646 A – ISDN primary rate interface E1 – unbalanced, 75 Ohm</td>
<td>⇒ STM-1e</td>
</tr>
<tr>
<td>• Keeps a record of approved cryptographic means and issues passports to all individually tested cryptographic means;</td>
<td>• J4647 A – ISDN primary rate interface – balanced, 120 Ohm</td>
<td>• Oscilloscope cart compatible with a large category of measurement tools</td>
</tr>
<tr>
<td></td>
<td>• J2905 B – ISDN BRI S/T and U interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• J3759 B – WAN E3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• J2912 B – OC-3/ STM-1</td>
<td></td>
</tr>
</tbody>
</table>

Necessary approximated costs (EURO) 90 000

#### 2. Mobile laboratory for network analysis and monitoring (TEMPEST zoning and evaluation of the security of AIS)

<table>
<thead>
<tr>
<th>Justification</th>
<th>Available testing equipment</th>
<th>Necessary testing equipment</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Coordinates and controls the protection against parasitic electromagnetic emissions from technical devices processing, storing and transmitting classified information;</td>
<td><strong>TEMPEST zoning and EMI measurement equipment:</strong></td>
<td><strong>Common use for TEMPEST zoning, EMI measurement equipment and evaluation of the security of AIS</strong></td>
</tr>
<tr>
<td></td>
<td>• Generator up to 4 GHz</td>
<td>• Automobile Van (Bus type)-2 working places, equipped with</td>
</tr>
<tr>
<td></td>
<td>• Spectrum analyzer up to 3 GHz</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Two wireless- B</td>
<td></td>
</tr>
</tbody>
</table>

Common use for TEMPEST zoning, EMI measurement equipment and evaluation of the security of AIS
| access point enabled to connect with PCs | 1. TEMPEST zoning equipment:  
| Two calibrated antennas up to 2 GHz | - Generator up to 26.5 GHz  
| Pre-amplifier up to 18 GHz. | - Spectrum analyzer up to 26.5 GHz  

Two calibrated antennas up to 2 GHz  
Pre-amplifier up to 18 GHz.

| Necessary approximated costs (EURO) | 430 000 |

3. RFD-F/A-100 anechoic chamber for measuring electromagnetic emissions

<table>
<thead>
<tr>
<th>Available testing equipment</th>
<th>Necessary testing equipment</th>
</tr>
</thead>
</table>
| - The coordination and control of the protection against spurious electromagnetic emissions from technical devices processing, storing and transmitting classified information involves tests for | - The purchase of a high precision system with specialized software:  
- Test Receiver  
  Frequency range 100 Hz to 22 GHz  
  IF bandwidths (RBW) 10 Hz to 500 MHz in steps of ½/5  
  Full-featured test receiver or spectrum analyser operating modes selectable  

| Laboratory for microwave measurements  
| A set of calibrated antennas from 100 Hz to 18 GHz  
| Spectrum analyser with lower sensitivity (max 115 dBm)  
| Special software has been elaborated for the purpose |
electromagnetic emissions in an anechoic chamber and the process is controlled by GPIB interface

- Signal generator up to 20 GHz
- Function arbitrary waveform generator – 15 MHz
- Vector network analyser up to 20 GHz
- Power meter – 18 GHz
- Turn table
- Antenna mast with automatic change of polarization

<table>
<thead>
<tr>
<th>Noise figure &lt;3 dB typ. (up to 2 GHz)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result memory for 500 000 samples (analyser mode) or 250 000 measurement values (receiver mode, one trace)</td>
</tr>
<tr>
<td>Built-in controller with operating system WindowsNT</td>
</tr>
</tbody>
</table>

- **RF Preselector**
  
  Versatile filters:
  - 11 highpass and 7 lowpass filters
  - 9 bandpass filters from 40 MHz to 2 GHz
  - 4 highpass filters from 2 GHz to 22 GHz

  Switchable 10/20/30 dB preamplifiers for maximum sensitivity

  Balanced input (0.3 kHz to 50 kHz) with selectable impedance

  Built-in comb generator up to 2 GHz

  - GPIB cables, RF cables, software and other equipment for test measurement
  - Spectrum analyser with -150 dBm sensitivity, 26.5 GHz
  - Oscilloscope cart compatible with a large category of measurement tools
  - 2 x UPS – 5 KVA

Necessary approximated costs (EURO) 400 000

### 4. Security training auditorium

<table>
<thead>
<tr>
<th>Available equipment</th>
<th>Necessary equipment</th>
</tr>
</thead>
<tbody>
<tr>
<td>- CISD conducts training of security officers for AIS or networks</td>
<td>- 2 x Notebook</td>
</tr>
<tr>
<td>- Auditorium with 25-seat</td>
<td>- 25 x PCs</td>
</tr>
<tr>
<td>- Whiteboard</td>
<td>- 2 x Servers</td>
</tr>
<tr>
<td></td>
<td>- Powerful LaserJet Printer</td>
</tr>
<tr>
<td>Necessary approximated costs (EURO)</td>
<td>80 000</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>--------</td>
</tr>
</tbody>
</table>

**Total Necessary approximated costs (EURO) 1 000 000**

The CISD-MoI officers, who work on the problems of classified information protection, have high qualification, but bearing in mind the dynamics in the spheres of technology and the related regulations, there is necessity of training courses for operation with the specialized facilities, used in specific measurements and analyses, and also of courses for introduction to EU standards in this field, with respect to their enforcement in practice.