Council of the
European Union

Brussels, 24 May 2018
(OR. en)

5602/06
ADD 1 DCL 1

SCH-EVAL 11
COMIX 76

DECLASSIFICATION

of document:	5602/06 ADD 1 RESTREINT UE/EU RESTRICTED
dated:	8 December 2005
new status:	Public
Subject:	Answers to the additional questionnaire addressed to the new Member States related to - Schengen Information System - Prior consultation

Delegations will find attached the declassified version of the above document.

The text of this document is identical to the previous version.

COUNCIL OF
THE EUROPEAN UNION

Brussels, 8 December 2005

5602/06
ADD 1

RESTREINT UE

SCH-EVAL 11
COMIX 76

NOTE	
from :	the Cyprus delegation
to:	the Schengen Evaluation Working Party
No. prev. doc. :	9820/1/05 REV 1 ADD 1 SCHEVAL 36 COMIX 380
Subject :	Answers to the additional questionnaire addressed to the new Member States related to - Schengen Information System - Prior consultation

I. Schengen Information System

Note : Questions included in the following chapter are based on the current SIS, but are equally valid in relation to SIS II.

1.1. Legislative and regulatory provisions adopted or to be adopted to set up the national system.

Relevant amendment of Police law 2004 is under way. The Convention implementing the Schengen agreement has been ratified by "Ratification Law 35(III/2003).

1.2. Have you already made preparations on the practical modalities or created National Information Systems for the purpose of issuing and accessing the following categories of alerts:

a) alerts on persons who should be refused entry to the Schengen area;
b) alerts on persons wanted for arrest (in view of surrender or extradition);
c) alerts on persons to ensure protection or prevent threats;
d) alerts on persons wanted for judicial procedure;
e) alerts on persons and objects for discreet surveillance or specific checks;
f) alerts on objects for seizure or use as evidence in criminal proceedings.

Are these systems set up with the future data structure of the SIS II in mind?
If yes, what is the level of progress achieved?
If not, please describe the relevant projects/plans.

The IT Branch of the Cyprus Police in co-operation with other departments and services is currently putting together a plan to migrate the existing Alert/Stop List data to the National Information System. The existing database contains alerts on persons of category (a),(b),(c),(d) and (e) .

Organizational conditions

1.3. Geographical location of the future access points or national interfaces of the SIS II (if known).

Geographical Locations:

- Larnaka airport
- Pafos airport
- Lemesos Port
- 5 locations for Marinas. (Agia Napa, Larnaka, Agios Rafail, Pafos, Latsi)
- Ministry of Foreign Affairs
- Police (Police Headquarters, Aliens and Immigration Department. It should be noted that all the Police Districts and Police Stations have the necessary infrastructure for future connection, if it will be decided)
- Customs & Excise Department
- Civil Registry and Migration Department

1.4. Describe the structure, hierarchy and organisation of the future SIS II national office.

The Police IT Branch has the responsibility for the installation of NSIS and the head of the IT Branch will be the Head of the NSIS. The structure will be as follows:

-1 Manager
- 1 System Engineer
- 1 Network Manager
-1 Security Officer
-,1 Database Manager
- 4 Senior Programmers

- 2 Programmers
- 2 Technicians
- 20 Data Entry Officers
- 1 Store keeper.

1.5. General presentation of the organisation of the services responsible in future for police functions in relation to the SIS II.

In Cyprus there is a single National Police Service. Section 6 of Police Law of 2004 (Law 73(I)/2004 as amended by Law 94(I)/2005) empowers the Police to act throughout the territory of the Republic for the maintenance of law and order, the preservation of peace, the prevention and detection of crime and the apprehension of offenders. For the performance of these duties, its members are entitled to carry weapons.

The Cyprus Police is under the political supervision of the Ministry of Justice and Public Order. The organization of the Police is based upon a hierarchical structure..The Chief of Police has the overall responsibility for the performance of all police duties, including border control.

The Police Department responsible for the NSIS is the IT Branch, which is located within the Police Headquarters in Nicosia. The Head of the IT Branch reports to the Director of the Research & Development Department, Police Headquarters.

1.6. Which tasks under national law shall necessitate access to SIS II by the judicial authorities?

Same as answer 1.1

1.7. List of services or authorities which will be authorised to process SIS II data including access to it.

- Police (Police Headquarters, Aliens and Immigration Department. It should be noted that all the Police Districts and Police Stations have the necessary infrastructure for future connection, if it will be decided)
- Ministry of Foreign Affairs
- Customs & Excise Department
- Unit for Combating Money Laundering (MOKAS)
- Civil Registry and Migration Department

Technical conditions

1.8. How many terminals are or will be made available for input and consultation of data by:

(a) Law enforcement services, including those with a control function
(b) The border control authorities;
(c) Diplomatic missions and consular posts;
(d) The authorities responsible for aliens and asylum;
(e) Customs authorities
(f) Others ?

(a) Police, Customs & Excise Department
(b) 37 Larnaka Airport (Police Aliens & Immigration Department-A.&I.D.)
10 Pafos Airport (Police A.&I.D.)
12 Lemesos Port (Police A.&I.D.)
5 Marinas (Agia Napa, Larnaka, Agios Rafail, Pafos, Latsi)- (Port &Marine Police)
(c) 1 at Ministry of Foreign Affairs
(d) 1 at Civil Registry & Migration Department (Asylum Office)
(e) 1 at Customs & Excise Department
(f) 10 at SIRENE Office
It should be noted that the NSIS is designed to connect up to 1000 end users.

1.9. Presentation of the computer architecture of national systems which will be connected to the SIS II.

Multi-tier Architecture
First-Tier - Database Server
Second-Tier - Application Server
Requests and responses are transmitted over the Network from the client Workstations. Two clusters, each cluster has its own external shared storage.
Third Tier - Client Workstation
Interface sessions from and to the user take place on the client Workstation. This is achieved with the use of Web Browser.

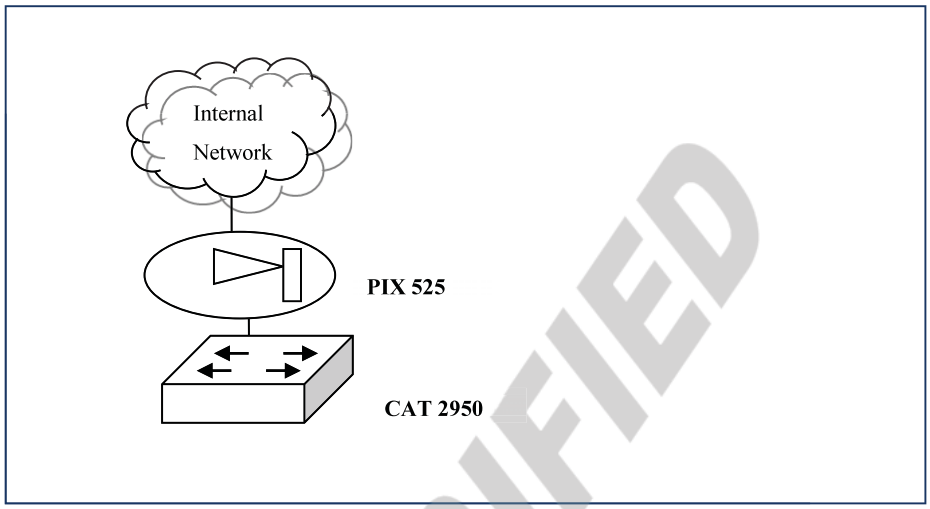
The system and Application environment Configuration is as follows:
DATABASE SERVERS : Sun Solaris, Veritas cluster, Oracle9i RDBMS.
APPLICATION SERVERS : Sun Solaries, Veritas cluster, Oracle9i AS
CLIENT WORKSTATIONS : Microsoft Windows XP Professional.

Cabling and Networking

The best quality Copper cable (CAT 5e) is used, and Fiber Optic connections. The system is connected to the Government Data Network (GDN). The Police Headquarters is connected to the backbone GDN Network with a 34 Mbps F.R. The system and application environment application is as follows:

DATABASE SERVERS: SUN SOLARIS, Veritus Clusters, Oracle 9i RDBMS
APPLICATION SERVERS: SUN SOLARIS, Veritus Clusters, Oracle 9i AS CLIENT WORKSTATIONS: Microsoft Windows XP Professional

Internet Security Protocol VPN between Main Headquarters and Remote Sites



1.10. Description of the future data flows between national systems and the SIS II in connection with input of data according to each of the aforementioned category of alerts

Future plans are under study.

1.11. Description of the future computer processing of SIS II data from the remote workstation of an end user.

Future plans are under study.

1.12. Does the national system allow for phonetic queries?

No.

1.13. How will the competent authorities on the ground have access to end-user terminals (by radio, only by telephone, via mobile terminals fitted in vehicles, only in person, only in writing)? Are there differences between the various national authorities?

Ground Services will have access to the system by radio and telephone. Other method of communication are under consideration.

1.14. Procedure planned to be followed by a user in the field to consult the SIS II database. Will the SIS II and the national system be consulted at one and the same time, or do both systems have to be consulted separately?

The procedure has not been decided yet, but both systems will be consulted at one and the same time

1.15. Volume of data to be transmitted to the SIS II database

Under study.

1.16. Have you already created a contingency centre/separate backup centre? If so please give further details about location, functions etc.

There is a contingency centre but there is no separate backup centre. The current location is the computer centre in the IT Branch in the Police Headquarters.. In the future, when the back up police system will be installed, a separate location of the backup centre will be considered.

1.17. Will checks be made of the switch between the backup and the operational system (BP 5.6.1)?

Under study.

1.18. What measures are you planning to take to guarantee 24/7 operations? How will the engineer support be organised?

Operation and engineer support will be on a 24/7 basis.

The existing Police Computer System and the future NSIS are designed to have 999.99 availability (5/9s). Also at the official entry points of Cyprus Police will install back up servers to guarantee 99.99% availability. A new UPS and a new generator have been installed.

1.19. How will the backup system be organised?

Will you take daily copies? On what media will backups be kept? If so describe the location and its protection. Will they be transported to other locations?
How will the media be labelled and protected during support? Will backup systems regularly be checked? Will restoration procedures be checked and tested? If so, how often?

The backup sub-system consists of one Sun Blade 150 Workstation and two L25 LTO Tape Libraries connected together. The software to perform backup is the Veritas NetBackup which gives fully functional backup and recovery. The NSIS Backup system will be set up in such a way so that if the main system fails it will take on automatically with zero time down.

The system backups are performed daily, weekly and monthly. The media will be labelled according to the system. For example, RDB000 means database backup, FOB001 means full backup, SYS000 means system backup and DEV000 means development backup. As soon as the policy is finalized and applied, the backups will be moved to another location. We haven't checked the backups yet, but we are planning to do so soon.

1.20. Have you already prepared an emergency plan relating to situations where it is impossible for users to search the SIS due to problems of the national systems or network inaccessibility? What are its main elements?

In case of emergency it is planned to use the facilities provided by the EU to re-direct the searches to CSIS.

1.21. How will the consular posts of your country access the SIS II?

This is under study.

Data

1.22. Are there any plans to introduce methods for collecting statistics on system down time?

Not currently, but this is under consideration.

1.23. Management/review of SIS II alerts

(a) How will deletion of the data be guaranteed if action has been taken in response to an alert?
(b) What kind of checks will be carried out?
(c) At what stage of implementation will an alert be deleted? (e.g. immediately after notification of an arrest, after notification of a person's whereabouts, after the reported discovery of an object, or after all measures have been taken, e.g. actual extradition, dispatch of documents to the place of residence, retrieval of the object)
(d) How will the authority responsible for central or local management carry out its duty of preventing the data files from becoming clogged with data (non-deletion of alerts after a hit)?
(e) What measures will be taken to cope with such a situation if it is detected?

No procedure for managing SIS alerts have been implemented yet.

1.24. Which concrete steps will be taken by the end-user when it is proven that there is a case in the SIS II of misused identity?

The end user will report the incident to the SIRENE Bureau who will perform the relevant procedure provided by Form Q.

Security

1.25. Security measures to ensure the control of future access to SIS II data? Measures put or which will be put in place to ensure that each user has access only to the categories of data for which he or she is authorised.

The access given to the end users will be controlled by the database, the application and the system login user-id and passwords. The access control will be managed by different categories and in the future plans will put in place a system that all inquiries and events will be locked. We will also implement a full auditing system.

1.26. What security measures at the future national systems (physical and logical security and security organisation)

The physical access will be controlled electronically and a future study will be carried out to view methods and procedures to provide a high level security

1.27. Control of physical access to the premises of the future national systems , where applicable including paper archives storage rooms.

Refer to answer of the Question 1.26

1.28. Level of protection and protection measures applied to computerised national applications – and in connection to this which special measures will be taken in relation to the SIS II application?

Refer to answer of the question 1.25

Training and information

1.29. Description of the specific training given to future operators and to those responsible for the national systems in future.

The Police users have gained an in-depth knowledge of all parts related to the national systems. They had a specific training on : 1) Overview of system operation, 2) Hands-on Network Management, 3) Introductory course on UNIX (Operating System), 4) Training on national applications and 5) Training sessions on email, operators' manual and incident control procedures.

1.30. Training and information for end users. In particular:

- **Will newly-recruited user (e.g. policemen) be given training in the use of SIS? If so, what will be the content of this training and how many hours will it last?**
- **Will continued training take place in the form of courses, seminars, conferences etc? If so, how many hours?**
- **If continued training will be provided, i.e. courses, seminars, conferences, how many hours.**

All Police users are trained at the Police Academy. The length of the training depends on the application they run. A continuing training e.g. seminars, and courses, is provided by the Police Academy. Also, all recruit officers will be trained in the use of SIS.

1.31. What measures are being or will be taken to ensure the level of competence of new users?

New users will be limited to access the application of the system that relates to their duties. New users will be trained appropriately.

1.32. Alert procedures for the judicial authorities and procedures following a hit:

(a) How will judges and public prosecutors be informed about the SIS (awareness of the SIRENE Bureaux, the role of the SIRENE Bureaux, differences between SIS and Interpol searches)? (by specific training, in the course of ordinary training, multiplier effect from trainers, publications, through specific brochures, through general public relations work)? Will they be informed regularly, just once or not at all? Are there regional differences?

(b) Will the future SIRENE Bureaux have any influence (by information and training measures)?

The judicial authority is an independent service of the Republic of Cyprus. However, close co-operation exists between the judicial authorities, the Attorney General Office, the Ministry of Justice & Public Order and the Police. For issues related to SIS, it is expected that judicial authority will closely co-operate with the SIRENE Bureau.

Regarding training of the judicial authority, this will be part of the national SIRENE training programme.

II. SIRENE (will certainly need to be updated on the basis of the result of the discussions of the SIS II legal proposals)

1.33. Have you already set up your SIRENE bureau? If yes, what level of progress has been achieved ? If no, please describe the relevant projects/plans.

The Cyprus SIRENE Bureau has been set up since 4 April 2005. Administratively, it is under the jurisdiction of the European Union & International Police Co-operation Directorate (EU&IPCD) of the Police Headquarters. Presently, the Bureau is staffed only by the Head of the Office, who participates in the monthly meetings of the Working Group SIS/SIRENE at Brussels. The Head of SIRENE Bureau also undertook the responsibility to promote the SIRENE establishment project.

Until now, the premises which will house the SIRENE Bureau have been located, within the vincinity of the Police Headquarters and within walking distance from INTERPOL and EUROPOL Offices. Reconstruction works are under way (re-wiring, installation of security system, refurbishment) . It is estimated the works will be completed by the end of April 2006. (The cost is estimated at about 80.000 euros.)

Organizational conditions

1.34. Geographical location of the future SIRENE Bureau.

The SIRENE **Bureau** is in the vicinity of the Police Headquarters, Nicosia and within walking distance from the Offices of INTERPOL and EUROPOL.

1.35. Administrative organisation of the future SIRENE Bureau and practical organisation of the work of the SIRENE Bureau (staff, administrations represented, day and night teams, specialisation of operators…). What about language skills availability? Will they all cover at least English and/or French during night time and on weekends? If not, what will they do with urgent information in foreign languages at those times?

The administrative organisation, as well as the precise practical organisation of the work of the SIRENE Bureau are under consideration. More specifically, draft plans have been prepared by the Head of the Office. There remains their examination with a view to approval by the Chief of Police. This is expected to be done in the near future.

The SIRENE **Bureau** is under the jurisdiction of the European Union & International Police Co-operation Directorate (EU&IPCD) of the Police Headquarters. (the organisational structure of EU&IPCD is attached to this document under APPENDIX A). Cyprus Police Organisational Structure can be found in APPENDIX B. The SIRENE Office Organisational Structure is under study.

Regarding language skills, it will be a pre-condition that all persons, who will staff the SIRENE Bureau shall have very good knowledge of English, as well as computer skills.. Some of the members of the SIRENE Bureau will also speak French and other European languages. As far as urgent information in foreign languages is concerned, other members of the Police who are available on 24/7 basis will be used. The requirements provided by the SIRENE Manual and Best Practices Catalogue will be taken into account for the recruitment for the Office.

1.36. Are you planning to hire civilian personnel?

Persons not belonging to any national authority
- **will such persons work on your premises?**
- **if so, what measures will apply/will these persons have the necessary clearance or certification?**
- **will non-disclosure/confidentiality agreements be made?**

SIRENE Bureau will be staffed by Police members. Also, Customs & Excise Department personnel, as well as members of the Legal Service will participate in the Office.

1.37. The limits of the respective spheres of competence of operators and end users.

Operators of the SIRENE Bureau will have full access to the SIRENE System. Also, they will have right of entry to other Police and governmental databases. The access of the End –Users will be limited to the relation of their duties.(cf 1.3.1 above)

It should be noted that it has not been decided yet who will have the responsibility for data entry, modifications, removals, etc of the SIRENE System. Decision will be taken in the near future.

1.38. What practical steps have been or will be taken to issue alerts on persons wanted for arrest (in view of surrender or extradition) ? Do agreements exist with the judicial authorities, particularly with a view to ensuring that SIS alerts take priority over Interpol alerts?

A 24/7 basis co-operation will be established between the National Contact Point, at the Ministry of Justice and Public Order, as well as with the Prosecution Office of the Police Headquarters and the Attorney General's Office,. (Law Office of the Republic)

All necessary arrangements will be made so all the SIS alerts will have priority over those from INTERPOL.

1.39. How will the activities related to alerts for the purpose of refusing entry and Articles 5 and 25 of the Convention be performed?

(a) Which authorities in your country will issue the alerts for purposes of refusing entry?

The Director of Civil Registry and Migration Department.

(b) Which authority will perform the role of the national SIRENE Bureau with regard to these alerts ? Will clearly defined channels of communication be in place between the national authorities involved?

Regarding the refusing entry alerts, the Police Aliens and Immigration Department will have the responsibility for their performance.

Since the Aliens and Immigration Department and SIRENE Bureau are Services of the Police, there will be matter-of-course, clearly defined channels between them. It should be noted that all Services involved in refusing entry procedure co-operate closely and no communication problems have been faced until now.

(c) What measures will be taken as regards the availability for the SIRENE bureau of background information (for example, a decision on expulsion/ban on entry) which is not recorded in the SIS?

Apart from the access to the SIRENE Bureau System, Operators of the SIRENE Bureau will have right of entry to other Police and Governmental databases for the retrieval of background information, eg. decision on expulsion/ban on entry, work permits, national stop- list, etc.

(d) Which national authority will liaise with the Schengen partners for purposes of sending and receiving of requests for consultation under Article 25 of the Convention?

The SIRENE Bureau.

1.40. The Sirene Bureaux' position and margin for manoeuvre at national level

(a) Will the Sirene Bureau have the possibility to directly consult and enter data in the national police system when running SIS searches, or initiate procedures for this to be done, (such as on indications concerning an abductor in an alert on a missing minor)? If not, are steps being taken to this end? Unclear.

Although nothing has been agreed so far, it is expected that as the SIRENE Office is under the jurisdiction of the Cyprus Police, it will have access to the Police Computer Data and will investigate and do searches in co-operation with the relevant Police Departments.

(b) Will the Sirene Bureau be able to access and enter data into other databases (vehicle registration databases, aliens' registers, population register), is there coordinated and effective cooperation with the corresponding departments?

Operators of the SIRENE Bureau will have access to other Police and Governmental databases only for the retrieval of information. No direct data entry or modifications of the data registered in those databases will be done by SIRENE Operators.

(c) Will the Sirene Bureau have the possibility to give instructions or will it have any other ways of influencing cooperation? Does national authorities training cover the future Sirene Bureau?

Operators of SIRENE Bureau will have close co-operation with all other Police and Government Services. Since SIRENE Bureau is part of the Police and its structures, the necessary co-operation and coordination with other Police Departments/Units/Districts at a high and a priority level is secured as an indispensable part of the functioning of the Police . The SIRENE Bureau, as the central SIRENE authority will be able to inform and alert simultaneously both the top hierarchy of the other Services as well as the officials directly involved , so that information and action/responses can be immediate. This will build on the existing excellent co-operation, coordination and communication with other Government Services.

Regarding the national authorities training, this will be offered by the Cyprus Police Academy in co-operation with other Government Services involved in SIRENE issues and the Police IT Branch. It should be mentioned that Police end-users have already been trained in the national computer systems.

(d) Will the Sirene Bureaux be empowered to conduct investigations (?) or act as coordinators? (such as in Articles 39 and 41).

The SIRENE Bureau will be the national coordinator /contact point for police co-operation and exchange of information. Investigations will be carried out by the relevant national law enforcement authorities i.e. Police, Customs & Excise Department and Unit for Combating Money Laundering (MOKAS).

Technical conditions

1.41. Technical arrangements made to enable to operate the future SIRENE Bureau without interruption in exceptional situations such as natural disasters, power cuts, disturbance or interruption of traditional telecommunications systems, etc.

All the necessary measures will be taken in order to secure the uninterrupted operation of the SIRENE Bureau (UPS systems, radio, alarms, back-up, etc. are planned to be installed)

Data

1.42. Follow-up action

(a) Will hits following alerts be recorded manually or automatically ?
Automatically.

(b) If they will automatically be recorded, how this will be done?

All the hits will be recorded in the system for future use. The SIRENE Bureau will be notified by the system automatically for their response.

(c) Will the actions taken after a hit occurred, f.i. the results of an investigation, be recorded? If so, this will be done centrally or locally? How long the results of an investigation will be retained?

Regarding the issue of the recording and the retention of the results of investigations, the provisions of the national legislation and the Police Standing Orders will be followed.

Data protection and other legislation

1.43. Legislative and regulatory provisions adopted or to be adopted to set up the SIRENE Bureau, including subsequent legislative measures.

Articles 92-101 of the Convention implementing the Schengen Agreement have been adopted by the Republic of Cyprus through the Law Ratifying the Treaty of Accession of Cyprus to the EU (Ratification Law 35(III)/ 2003) However, the establishment and function of the National SIRENE Bureau will be provided for in a separate law that will implement and in corporate into national law and practices the provisions of the aforementioned Articles. Thislaw is under preparation.

1.44. Foreseen security measures at the future SIRENE Bureaux (logical and physical security, security organisation)

The logical and physical security of the SIRENE premises will be consistent with the SIRENE Manual and the Best Practices Cataloque. The construction plans include the following measures:

- security perimeter
- physical barriers
- external walls of solid construction
- access doors with access cards
- monitoring of entries and CCTV system
- fire, heat and smoke detectors
- 24/7 surveillance

1.45. Control of physical access to the premises of the future SIRENE Bureau, where applicable including paper archives storage rooms.

Access will be restricted to authorised personnel, via use of individuals access cards and codes.

All the archives will be stored electronically, in separate locations and where paper is necessary a strong room will be used within the premises. Access to the strong room will only be possible for authorised personnel.

The control of physical access to the SIRENE premises will be consistent with the SIRENE Manual and the Best Practices Catalogue. The construction plans include the following measures:

- security perimeter
- physical barriers
- external walls of solid construction
- access doors with access cards
- monitoring of entries and CCTV
- fire, heat and smoke detectors
- 24/7 surveillance

1.46. Level of protection and protection measures applied to computerised police applications – and in connection to this which special measures taken or to be taken in relation to the Sirene application

The following security and protection measures are currently applied to computerised Police applications:

- Use of Government Data Network
- Use of firewalls
- User IDs and passwords
- Different level of access/application
- Audit trail
- Secure installation sites

All the necessary measures provided by the SIRENE Manual and the Best Practices Catalogue will be adopted.

1.47. Who is in your country the national supervisory authority regarding data protection issues?

The Commissioner for the Protection of Personal Data.

1.48. Measures taken or which will be taken to ensure that SIRENE files are destroyed after withdrawal of the alerts to which they relate. Who will be responsible for controlling implementation?

This will be done according to the national legislation. The Police Standing Order 1/45 provides the rules and procedures for the destruction of files and data.

Education and information

1.49. Description of the specific training given or planned to future operators and to those responsible for the SIRENE Bureau in future.

Operators and Officers of the SIRENE Office will be trained on the following subject:

- SIRENE theory and practice.
- National Law
- Schengen Acquis.
- SIRENE Manual
- Best Practices Cataloque.
- Use of Computers and INTERSIRENE.
- Handle of HITS.
- Management procedures for the implementation of the S I S .
- Seminars and Education in Cyprus and abroad.
- Study Visits in other Member States where SIRENE Bureaux already exist, i.e. Austria, Greece, France, Italy .

1.50. Training and information for end users. How will you organise the training when the SIS is implemented ?

Police end-users have already been trained at the national computer systems. The length of the training depends on the application they run. A continuing training e.g. seminars, and courses, will provided by the Police Academy. Also, all recruit officers will be trained in the use of SIS

1.51. What measures are being taken to ensure the level of competence of new users?

Before new users will be allowed access to the SIRENE system they will be thoroughly trained. Training and on-the-job supervision will be continuous until the Head of the SIRENE Bureau will be satisfied that they will have reached a level of competence permitting access and use of SIRENE without supervision.

1.52. How will police officials on the ground be informed about the SIS and the SIRENE Bureaux (by specific training, in the course of ordinary police training, multiplier effect from trainers, articles published in police journals, through specific brochures, through general public relations work)?

Police officials on the ground will be informed about the SIS and the SIRENE Bureau by:
- Training programmes at the Police Academy (including recruit officers)
-regular training for trainers / area supervisors
- Police Standing Orders
- Weekly Orders of the Chief of Police
- Police Bulletins
- Special Seminars/TAIEX workshops and Lectures at Headquarters and at District level.
- Articles in the Police magazines

1.53. Which procedures have to be followed at the future SIRENE Bureaux once informed about a misused identity alert?

The form Q procedure will be followed.

1.54. What procedures will be put in place following a hit?

The subject is under study and it will be consistent with the existing national legislation, Police Standing Orders and the SIRENE Manual..

1.55. Relationship of the SIRENE bureau with prosecuting authorities

A 24/7 basis co-operation will be established between the SIRENE Bureau and the National Contact Point at the Ministry of Justice and Public Order, as well as with the Prosecution Office of the Police Headquarters and the Attorney General's Office.(Law Office of the Republic) It should be noted that a Prosecution Office operates within the Police which is in direct contact with the Attorney General's Office.

III. Under chapter "Visa"

INFORMATION ON VISA RELATED ISSUES WILL BE PROVIDED AT A LATER STAGE

1.56. What provisions have been made to ensure that permanent consular posts will only issue Schengen visas in the future?

1.57. Is any specialised training given in the detection of false documents?

1.58. Are there any manuals of specimen documents to check that the documents presented are genuine?

IV. Prior Consultation

1.59. How are other States consulted? What technical means are implemented?

1.60. What is the estimated response time for consultation?

1.61. Under which circumstances do the consuls of your country consult their central authorities?

1.62. What criteria are applied?

1.63. Under which circumstances do other States consult them? (What is the number of national and international consultations?)

Do you intend to include third countries in Annex V B for prior consultation? How many?

APPENDIX A

CYPRUS POLICE
Organisational Chart of the European Union & International Police Cooperation Directorate