

GENERAL SECRETARIAT OF THE COUNCIL <i>Private Office</i>		Brussels, 30 June 2000 SN 3328/1/00 REV 1

NOTE FOR THE PERMANENT REPRESENTATIVES COMMITTEE

Subject: COUNCIL SECURITY PLAN

I. Objectives

- To establish the future security policy of the Council with a view to:
 - ❑ providing a safe and secure environment for the staff of the General Secretariat of the Council (GSC) and for all Council activities, in particular those related to the common European security and defence policy (ESDP)
 - ❑ establishing a coherent security approach, based on clearly defined standards and procedures, to cover personnel, physical and information technology (IT) security
 - ❑ providing a framework which will facilitate the conclusion of security agreements as necessary.

  To define specific security programmes identifying the measures to be taken so that the GSC can meet its security objectives.

-   To establish audit and review procedures to ensure that the security programmes can be adjusted to respond to changes in security requirements.

II. GSC Security Policy

The GSC security policy and its implementation instruments must provide a framework to ensure:

- the protection of staff and other occupants of the buildings, of property, assets and resources
- the confidentiality of classified information and the availability and integrity of all information kept or produced by the institution in whatever form
- the continuity of the Council's activity.

On the basis of this security policy, standards, procedures and practices, commensurate with the value of the information or physical assets they are meant to protect, will be defined. When applied, the policy will provide all individuals concerned with a clear understanding of their responsibility and accountability.

A draft security policy for the GSC will be circulated as document SN 3328/00 ADD 1. The Secretary General will adopt the GSC security policy.

III. Lines of action

1. General comments

Improving the overall level of security at the Council is a large-scale exercise, which can only be carried out in steps and which requires action - in most cases at considerable cost - in several areas:

- ❑ buildings and infrastructure
- ❑ information and telecommunication networks and equipment
- ❑ legislative and regulatory framework
- ❑ administrative structures and organisation.

Within this general programme, priority has been given to measures designed to respond to ESDP requirements for a secure environment, which would guarantee the protection of

classified information. Where necessary, pragmatic interim solutions are being considered to allow the necessary flow of relevant information.

2. Buildings and infrastructure

A. The Kortenbergh building

The building is currently occupied by Commission services and will be vacated at the end of July. Occupation of the building by the GSC is foreseen by the end of the year for one section (K-150) and by early 2001 for the remaining part (K-158). Extensive work is needed to provide a secure environment with installations and equipment up to the standards required for security agreements. Refurbishment and re-distribution of space in order to adapt it to GSC needs are also necessary. Work on the building is planned to start in August.

A specialised security engineering firm, with NATO security clearance, will assist the GSC in the implementation of the project; it will develop the technical specifications for the security - related measures and provide the corresponding cost estimate.

(a) Physical protection

The GSC has adopted the following general approach:

- ❑ the building will be reinforced to compensate for the fact that it lacks a perimeter (which, from a security point of view, is a drawback); measures such as reinforcement of walls/windows at ground level, 'shatter proofing' at the higher levels, hi-tech camera equipment, specialised lighting, etc. will be taken to this effect;
- ❑ within the building, security levels will be differentiated according to need; particularly sensitive areas will be protected to higher standards and will be equipped with access control with local intelligence;
- ❑ internal access flow will be designed to prevent direct access to the different floors from the garage;
- ❑ the building will be equipped with an access control system allowing for pinpoint access authorisation/denial according to pre-defined user profiles;
- ❑ in order to limit 'contamination' of the secured areas by non-screened individuals, the cafeteria

will be positioned in a separate zone;

- ❑ all equipment used for security purposes (i.e. containers for classified documentation, shredders etc.) shall be approved by the GSC security office, which will use lists of equipment approved by Member States for the protection of classified NATO/WEU material;
- ❑ special measures will be taken to protect the building from external and internal electronic eavesdropping, as well as from sabotage and malicious wilful damage; the Belgian authorities will assist the GSC and will ensure that the building is "technically secure".

(b) Procedures

The 'flexibility' in applying security procedures which has hitherto existed at the GSC cannot be carried over into the secure environment. While common sense will prevail, the environment dictates that security cannot be sacrificed to expediency.

Specific procedures and practices to be applied in the Kortenbergh building are being drafted and will govern all aspects of security associated with such an environment.

(c) IT Security

Within the comprehensive IT security policy which is currently being defined (see point 3 below), priority has been given to fulfilling the essential requirements of the Kortenbergh building, because of the need to ensure that the units working there will be immediately operational. The following priority requirements have been identified:

First phase (second half of 2000)

- ❑ First deployment of a protected e-mail system (commercial off the shelf public key infrastructure (PKI) and ciphering technology) for exchanging sensitive documents internally and with a limited number of external recipients.
- ❑ Training and awareness programmes (limited to the users more closely concerned with security issues).
- ❑ Setting-up of the unclassified and classified networks in K-150 (cabling and systems).
- ❑ Setting up of secure telecom infrastructure (secure telephone and data links with the Justus Lipsius building).

- ❑ Procurement of secure IT office equipment (servers, personal computers, printers, ...).
- ❑ Creation of the COMCEN in the Kortenbergh building.
- ❑ Creation of the CORTESY antenna and the hub for the defence network.
- ❑ Deployment of a defence network connecting the Secretariat to the Ministries of Foreign Affairs, Defence and Chiefs of Defence headquarters of the EU Member States.
- ❑ Provisional risk assessment and interim accreditation of targets of evaluation (classified networks, network boundaries protection, standard office automation suites, ...).

Second phase (from January 2001, during refurbishment work in K-158)

- ❑ Final risk assessment and accreditation of the various targets of evaluation
- ❑ Extension of the public key infrastructure to all users in the departments most concerned by security issues.
- ❑ Deployment of the secure internal network for voice, fax and e-mail exchange between departments.
- ❑ Partial deployment of the network for monitoring/management of crises (possibly including secure videoconferencing links).
- ❑ Raising the IT baseline protection of the overall IT infrastructure of the Secretariat by:
 - ❑ improvement of the availability of the unclassified network
 - ❑ improvement of the protection of e-mail exchanges with the external world and of Internet access.

❑ *Third phase (as soon as the K-158 is ready for occupation)*

- ❑ Setting up the unclassified and classified networks in the K-158 building (cabling and systems).
- ❑ Extension of the secure inter-departmental network (secure phones, fax and e-mail).

B. The Justus Lipsius building

General security of the Council at the Justus Lipsius (and to a lesser extent in Frère Orban) needs urgent upgrading.

A preliminary survey by the head of the Security Office has identified a number of weaknesses,

which require the GSC to:

- ❑ establish general security procedures, to be implemented under the responsibility of the Security office
- ❑ define and apply a coherent approach to physical security for sensitive areas
- ❑ define clear and structured procedures for accreditation and access
- ❑ discipline access by delegations
- ❑ raise the level of security in delegations' offices
- ❑ ensure control over third party activities at Council buildings
- ❑ provide protection against potential activity – by human or electronic means - by foreign intelligence agencies
- ❑ increase staff awareness of elementary principles and procedures with regard to the handling of classified material
- ❑ improve the level of expertise of security staff to meet the challenges imposed by the Council's new needs
- ❑ increase IT security.

Those elements which are relevant to the conclusion of security agreements have been given priority. They are being addressed with the competent services, in order to correct immediately the most obvious shortcomings. In this context, measures to guarantee the security of movement of people and documents between the buildings, as well as the possibility of securing a meeting room, are also being studied.

Other more structural changes will be addressed as part of a planned process and will be implemented accordingly.

3. IT Security

IT security must - as a general objective - provide an assurance of availability, confidentiality and integrity of information at all times.

This requires the definition of an IT security concept, which - on the basis of recognised good practices - identifies the systems, the organisation model and the equipment/infrastructure which

fulfil the requirements of the Council. Specific standards and procedures will have to be defined in detail in a subsequent phase, during which an exercise of risk assessment and identification of protection profiles will be carried out. A more precise cost assessment will be made at that point.

A draft IT security concept for the GSC will be circulated as document SN 3328/00 ADD 2. Initial and provisional cost estimates for implementation of the required IT security measures will be included.

As a prerequisite for implementation a number of organisational issues should be addressed:

- ❑ designation of the "IT security accreditation authority" by the Secretary General
- ❑ creation of INFOSEC capabilities with appropriate staffing
- ❑ review of the organisation of the IT division
- ❑ setting up of an internal "Security management forum" responsible for controlling, co-ordinating and reviewing the enforcement of security policies, under the chairmanship of the head of the Security office and with the participation notably of the head of the IT division, the INFOSEC manager, legal advisers and IT users' representatives
- ❑ appointment of IT security correspondents in the various departments.

Adequate financial resources should also be made available.

Once the organisational and financial prerequisites are fulfilled, the deployment of IT infrastructure can be planned in detail.

4. Legislative and regulatory framework

The higher level of security required to protect information under the ESDP makes it necessary to amend existing legislation or to adopt new texts.

(a) Present situation

The following texts, currently in force, are relevant to the protection of classified information:

- ❑ Decision n° 24/95 of the Secretary General of the Council on measures for the protection of classified information applicable to the General Secretariat of the Council
- ❑ Decision n° 433/97 of the Secretary General of the Council on the screening procedure of staff responsible for the functioning of the CORTESY system
- ❑ Council Decision of 27 April 1998 relating to the procedures whereby officials and employees of the General Secretariat of the Council may be allowed access to classified information held by the Council (98/319/EC) (OJ L 140 of 12 May 1998, p.12)
- ❑ Decision n° 530/99 of the Secretary-General of the Council of the European Union on the administrative procedures for implementing the Council Decision on access to classified information.
- ❑ Council Decision 93/731/EC of 20 December 1993 on public access to Council documents (OJ L 340 of 13 December 1993, p.43)
- ❑ Council Decision 2000/23/EC of 6 December 1999 on the improvement of information on the Council's legislative activities and the public register of Council documents (OJ L 9 of 13 January 2000, p.22).

(b) Proposed changes

The GSC proposes to replace the Secretary General Decisions of 1995 and 1997 and the Council Decision of 1998 by a new Council Decision covering all relevant measures to protect classified information, the security screening of personnel and the handling of classified information, whether on paper or through IT systems and networks ("Security regulations"). A draft will be circulated as soon as possible.

The proposed decision provides inter alia for the setting up of a consultative security committee chaired by the Secretary General. Its mandate would be to examine all questions related to the protection of classified information (including IT security).

Administrative implementing measures should continue to be adopted by the Secretary General. The SG Decision of 1999 will need to be adjusted in accordance with the new decision.

As regards public access to documents and the public register of Council documents, proposals have been tabled in Coreper to amend both decisions in order to exclude from their scope documents concerning security and defence matters. A similar exception should be included in the proposed regulation on transparency currently under discussion. The possibility of establishing

specific rules to cover police and judicial co-operation is being studied.

(c) New texts

- ❑ Draft framework Decision on the protection under criminal law of classified information. The Council Legal service suggests a decision based on article 34 paragraph 2, point b) of the TEU, which would ensure that Member states apply to breaches of secrecy the same criminal law rules they apply under article 194 of the Euratom Treaty. A draft to this effect will be circulated as document SN 3328/00 ADD 3.
- ❑ Security arrangements with Member states and NATO. Whilst permanent security agreements are being negotiated, interim arrangements should be prepared and introduced as soon as possible. This could be done through an exchange of letters, following the precedent of the GSC/WEU agreement of 15 April 1999.
- ❑ Coreper decision setting up an ad hoc working party with the specific time-limited mandate to examine the draft "Security regulations" decision mentioned above under point (b) and any other relevant legal texts.
- ❑ Other issues to be examined:
 - ❑ need to ensure that developments in the ESDP area are taken into account in the "draft regulation on the protection of personal data by Community institutions and bodies", currently under examination;
 - ❑ requirement for new rules and procedures governing relations with other EU institutions as regards the exchange of information and the protection of classified information: possibly to be covered by an interinstitutional agreement;
 - ❑ consequences of the recent framework agreement between the Commission and the European Parliament (notably its annex III);
 - ❑ review of current classification practice to ensure that only information that is sufficiently sensitive to require protection at a particular level receives that classification.

5. Administrative structures and organisation

A. Security office

Implementation of the new security policy requires restructuring and reinforcing the GSC Security Office. The main changes are the following:

- ❑ creation of new sections within the department: security engineering, information and investigation (including "staff vetting", currently dealt with outside the Security office; "electronic sweeping"; "audit of treatment of classified information");
- ❑ reintegration of the "Safety and prevention" section, currently attached to the building division.

This operation requires the reinforcement of the current staff complement of the Security Office and the recruitment of some specialists. It also requires the adoption by the Secretary General of a new decision replacing the Secretary general's decisions n° 920/97 and 921/97 concerning respectively the missions of the Security office and those of the Safety and prevention service.

Additionally, it is necessary to create INFOSEC capabilities with close links to the Security Office and to the IT Division.

B. Other administrative questions

From the point of view of organisation and administration, a number of areas require action by the GSC:

- ❑ recruitment procedures for security specialists, including IT security
- ❑ security screening for staff assigned to the Kortenbergh building who do not currently hold the appropriate security clearance ; this requires co-operation from Member States to ensure that procedures are carried out speedily

- ❑ analysis of the compatibility of the measures foreseen to improve the security of the GSC, including the measures for the protection of classified information, with Community acts on the protection of individuals with regard to the processing of personal data (art 286 EC)¹
- ❑ security awareness training for staff .

IV. Summary of decisions to be taken and timetable

1. *Decisions to be taken by the Council*

- ❑ **Adoption of framework Decision on the protection under criminal law of classified information. Target date: end of 2000.**
- ❑ **Adoption of the new Decision ("Security regulations"). Target date: end of 2000.**
- ❑ **Amendment of the Decisions concerning public access to Council documents and the public register of Council documents. Target date for adoption: as soon as possible.**
- ❑ **Regulation on transparency – subject to co-decision procedure – expected adoption date: first half of 2001.**

2. *Decision to be taken by Coreper*

- ❑ **Decision setting up the ad hoc working party mentioned above under point 4(c). Target date: July 2000.**

2. *Decisions to be taken by the budgetary authority*

- ❑ **(p.m.) Provide additional resources as required. Target date: autumn 2000 (rectifying letter) or first half of 2001 (supplementary and amending budget).**

¹ The GSC Data protection officer points out that measures such as access control, staff screening, video surveillance, control of access to computer systems are covered by the rules on data protection.

3. Decisions to be taken by the SG/HR and/or the DSG

- ☐ **GSC security policy (and attached standards, procedure and practices), after assessment of the compatibility of the new rules with those on the protection of personal data. Target date: September 2000.**
- ☐ **GSC IT security policy and IT security rules and procedures. Target date: autumn 2000.**
- ☐ **Administrative measures implementing the Council Decision ("Security regulations"). Target date for adoption: 2 months after adoption of the Council decision.**
- ☐ **Designation of the "IT security accreditation authority". Target date: September 2000.**
- ☐ **New Decision replacing SG Decisions n° 920/97 and 921/97 concerning respectively the missions of the Office of Security and those of the Prevention Service. Target date: autumn 2000.**
- ☐ **Reorganisation of the Security office and other administrative measures as required. Target date: July to December 2000 according to relative priority and availability of resources and staff.**
- ☐ **Allocation of available financial resources according to the priorities set for physical and IT security measures in the Kortenbergh and Justus Lipsius buildings. Target date: from July 2000 as required.**
- ☐ **Preparation and signature of interim security arrangements with NATO and the Member States. Target date: end of July 2000.**

5. Further action by the SG/HR and/or the DSG

- ☐ **Contacts with the other institutions (notably the Commission), possibly with a view to concluding an interinstitutional agreement on:**
 - ☐ **new rules and procedures governing the exchange of information and the protection of classified information**
 - ☐ **classification practices.**

6. Security agreements

- ☐ **with NATO**
- ☐ **with the Member States (as needed).**