ANNEX I

REQUIREMENTS AND TASKS OF COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTs)

The requirements and tasks of CSIRTs shall be adequately and clearly defined and supported by national policy and/or regulation. They shall include the following:

(1) Requirements for CSIRTs:

- (a) CSIRTs shall ensure a high level of availability of their communications services by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times. Furthermore, the communication channels shall be clearly specified and well known to the constituency and cooperative partners.
- (b) CSIRTs' premises and the supporting information systems shall be located in secure sites.
- (c) Business continuity:
  - (i) CSIRTs shall be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers.
  - (ii) CSIRTs shall be adequately staffed to ensure availability at all times.
  - (iii) CSIRTs shall rely on an infrastructure the continuity of which is ensured. To that end, redundant systems and backup working space shall be available.
- (d) CSIRTs shall have the possibility to participate, where they wish to do so, in international cooperation networks.

(2) CSIRTs' tasks:

- (a) CSIRTs' tasks shall include at least the following:
  - (i) monitoring incidents at a national level;
  - (ii) providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents;
  - (iii) responding to incidents;
  - (iv) providing dynamic risk and incident analysis and situational awareness;
  - (v) participating in the CSIRTs network.
- (b) CSIRTs shall establish cooperation relationships with the private sector.
- (c) To facilitate cooperation, CSIRTs shall promote the adoption and use of common or standardised practices for:
  - (i) incident and risk-handling procedures;
  - (ii) incident, risk and information classification schemes.