

(2) to consider the possibility of a financial support to this initiative on the basis of the financial interventions provided for educational activities by Council Decision of 9 December 1999 establishing a Community action programme in the field of civil protection⁽¹⁾ for the period 1 January 2000 to 31 December 2004 or by the said Council Decision establishing a Community mechanism to facilitate reinforced cooperation in civil protection assistance interventions,

(¹) OJ L 327, 21.12.1999, p. 53.

(3) to involve the candidate countries in its work.

(4) to consider, on expiry of this pilot phase and in the light of the results obtained, any initiative introducing long-term cooperation on civil protection training, for instance through the creation of a European civil protection college which would institutionalise the aforementioned network.

COUNCIL RESOLUTION

of 28 January 2002

on a common approach and specific actions in the area of network and information security

(2002/C 43/02)

THE COUNCIL OF THE EUROPEAN UNION,

RESPONDING TO

the Conclusions of the Stockholm European Council of 23 and 24 March 2001 that the Council together with the Commission will develop a comprehensive strategy on security of electronic networks including practical implementing action,

RECALLING

1. the Resolution of the Council of 30 May 2001 — eEurope Action Plan: Information and Network Security;
2. the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions — Network and Information Security: Proposal for a European Policy Approach;
3. the Communication from the Commission to the Council and the European Parliament — eEurope 2002: Impact and priorities;
4. the eEurope 2002 Action Plan endorsed by the Feira European Council of 19 and 20 June 2000;
5. Council Recommendation 95/144/EC of 7 April 1995 on common information technology security evaluation criteria⁽¹⁾;
6. the Council Recommendation of 25 June 2001 on contact points maintaining a 24-hour service for combating high-tech crime⁽²⁾;

(¹) OJ L 93, 26.4.1995, p. 27.

(²) OJ C 187, 3.7.2001, p. 5.

7. the Communication from the Commission on creating a safer society by improving the security of information infrastructures and combating computer related crime;

8. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data⁽³⁾;

9. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data⁽⁴⁾;

10. Directive 97/33/EC of the European Parliament and of the Council of 30 June 1997 on interconnection with telecommunications with regard to ensuring universal service and interoperability through application of the principles of open network provision (ONP)⁽⁵⁾;

11. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector⁽⁶⁾;

12. Directive 98/10/EC of the European Parliament and of the Council of 26 February 1998 on the application of open network provision (ONP) to voice telephony and on universal service for telecommunications in a competitive environment⁽⁷⁾;

(³) OJ L 8, 12.1.2001, p. 1.

(⁴) OJ L 281, 23.11.1995, p. 31.

(⁵) OJ L 199, 26.7.1997, p. 32.

(⁶) OJ L 24, 30.1.1998, p. 1.

(⁷) OJ L 101, 1.4.1998, p. 24.

13. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures ⁽¹⁾;

WHEREAS:

- (1) Networks and communication systems have become a key factor in economic and social development and their availability and integrity is crucial to essential infrastructures, as well as to most public and private services and the economy as a whole.
- (2) In the light of the increasingly important role played in the economy by electronic services, the security of networks and information systems is of growing public interest.
- (3) The security of transactions and data has become essential for the supply of electronic services, including e-commerce and online public services, and low confidence in security could slow down the widespread introduction of such services.
- (4) There is a need for individuals, businesses, administrations, and other organisations to protect their own information, data and communication systems by deploying effective security technologies, where appropriate.
- (5) The private sector, acting in a competitive market environment, and through its capacity to innovate offers a variety of solutions adapted to genuine market needs.
- (6) The complex nature of network and information security means that in developing policy measures in this field, public authorities must take into account a range of political, economic, organisational and technical aspects, and be aware of the decentralised and global character of communication networks.
- (7) Policy measures can be more effective if they are part of a European approach, respect the effective functioning of the Internal Market, build on increased cooperation between Member States and internationally, and support innovation and the ability of European enterprises to compete at global level.
- (8) A substantial body of legislation relevant to network and information security is already in place, notably as part of the Union's legal framework for telecommunications, electronic commerce and electronic signatures.

(9) There are legal requirements imposed on providers of telecommunications services to take appropriate technical and organisational measures to safeguard the security of their services; these measures shall ensure a level of security appropriate to the risk represented.

(10) The international standard ISO-15408 (Common criteria) has become a recognised system for defining security requirements for computer and network products and evaluating whether a particular product meets those requirements.

(11) The international standard ISO-17799 (Information technology — Code of practice for information security management) and similar national guidelines are becoming recognised practice for security management in private and public organisations.

(12) Internet infrastructure should permit a high degree of access to networks and services, and be managed and operated in a robust and secure manner, e.g. by the adoption of open standards and internet security protocols;

CONSIDERING, in line with Council Resolution of 30 May 2001 on the 'Europe Action Plan: Information and Network Security', that network and information security is about

- ensuring the availability of services and data,
- preventing the disruption and unauthorised interception of communications,
- confirmation that data which has been sent, received or stored are complete and unchanged,
- securing the confidentiality of data,
- protection of information systems against unauthorised access,
- protecting against attacks involving malicious software,
- securing dependable authentication;

THEREFORE ASKS THE MEMBER STATES

1. by the end of 2002 to launch or strengthen information and education campaigns to increase awareness of network and information security; to specifically target such actions at business, private users and public administrations; to develop such awareness raising actions closely with the private sector, including *inter alia* internet service providers, and to encourage private sector-led initiatives;

⁽¹⁾ OJ L 13, 19.1.2000, p. 12.

2. to promote best practices in information security management notably in small and medium sized enterprises based, where appropriate, on internationally recognised standards;
 3. by the end of 2002 to strengthen or promote the importance of security concepts as part of computer education and training;
 4. by mid 2002 to review the effectiveness of national arrangements regarding computer emergency response, which could include virus alert systems, with a view to strengthening, where necessary, their ability to prevent, detect, and react efficiently at national and international level against network and information systems disruption and attack;
 5. to promote the use of the common criteria standard (ISO-15408) and to facilitate mutual recognition of related certificates;
 6. by the end of 2002 to take significant steps towards effective and interoperable security solutions based on recognised standards where possible — which could include open source software — in their e-government and e-procurement activities, and towards the introduction of electronic signatures to allow those public services that require strong authentication also to be offered on-line;
 7. where they choose to introduce electronic and biometrics identification systems for public or official use, to cooperate where appropriate on technological developments and to examine any possible interoperability requirements;
 8. with a view to facilitating Community and international cooperation, to exchange information with each other and with the Commission on the bodies primarily responsible within their territory for network and information security matters;
- WELCOMES THE INCREASED FOCUS OF EUROPEAN RESEARCH ACTIVITIES ON SECURITY MATTERS;
- STRESSES THE NEED FOR MORE RESEARCH ACTIVITIES, IN PARTICULAR ON SECURITY MECHANISMS AND THEIR INTEROPERABILITY, NETWORK RELIABILITY AND PROTECTION, ADVANCED CRYPTOGRAPHY, PRIVACY ENHANCEMENT TECHNOLOGIES AND SECURITY IN WIRELESS COMMUNICATIONS;

WELCOMES THE INTENTION OF THE COMMISSION

1. in 2002 to facilitate an exchange of best practice regarding awareness-raising actions and to draw up an initial inventory of the various national information campaigns;
2. in 2002 to make proposals to reinforce the Community's dialogue and cooperation with international organisations and partners on network security, in particular on the impli-

cations of the increasing dependency on electronic communication networks; and in this context to propose, by the end of 2002, a strategy for a more stable and secure operation of the Internet infrastructure;

3. by the end of 2002 to propose adequate measures to promote the ISO 15408 (Common Criteria) standard, to facilitate mutual recognition of certificates, and to improve the process by which products are evaluated, i.e. by developing adequate protection profiles;
4. by the end of 2002 to prepare a report on technologies and applications of electronic and biometric authentication of identity with a view to improving the effectiveness of such systems, in particular through interoperability;
5. by mid 2002 to make proposals — after consultation with the Member States and the private sector — for the establishment of a cyber-security task force to build on national efforts to both enhance network and information security and to enhance Member States' ability, individually and collectively, to respond to major network and information security problems;
6. by the end of 2002, to explore, in collaboration with Member States, the possible options for mechanisms by which Member States and the Commission can exchange information and experience on their achievement of the objectives of this Resolution, taking into account the cross-pillar dimension of network and information security, and to explore how the private sector can be best involved in this exchange of information and experience;

WELCOMES THE INCREASED FOCUS OF EUROPEAN RESEARCH ACTIVITIES ON SECURITY MATTERS;

STRESSES THE NEED FOR MORE RESEARCH ACTIVITIES, IN PARTICULAR ON SECURITY MECHANISMS AND THEIR INTEROPERABILITY, NETWORK RELIABILITY AND PROTECTION, ADVANCED CRYPTOGRAPHY, PRIVACY ENHANCEMENT TECHNOLOGIES AND SECURITY IN WIRELESS COMMUNICATIONS;

CALLS UPON

- suppliers and service providers to strengthen security as an integral and essential part of their products and services;
- the European private sector suppliers and service providers and their representative groupings to participate more actively in international standardisation activities and organise themselves into appropriate fora to contribute to the objectives of this resolution.