***Changes to legislation:** There are currently no known outstanding effects for the Council Decision of 31 March 1992 in the field of security of information systems (92/242/EEC). (See end of Document for details)*

ANNEX

Summary of action lines
ORIENTATIONS FOR AN ACTION PLAN IN THE FIELD OF THE SECURITY OF INFORMATION SYSTEMS

INTRODUCTION

The action plan shall have as its objective the development of overall strategies aiming to provide users and producers of electronically stored, processed or transmitted information with appropriate protection of information systems against accidental or deliberate threats.

The action plan shall take into account and complement the world-wide standardization activities under way in this field.

It shall include the following lines of action:

— development of a strategic framework for the security of information systems;
— identification of user and service provider requirements for the security of information systems;
— solutions for immediate and interim needs of users, suppliers and service providers;
— development of specifications, standardization, evaluation and certification in respect of the security of information systems;
— technological and operational developments in the security of information systems;
— provision of security of information systems.

The action plan shall be implemented by the Commission, in close association with related actions in Member States and in conjunction with related Community research and development actions.

1. **Action line I — Development of a strategic framework for the security of information systems**

1.1. *Issue*

Security of information systems is recognized as a pervasive quality necessary in modern society. Electronic information services need a secure telecommunications infrastructure, secure hard- and software as well as secure usage and management. An overall strategy, considering all aspects of security of information systems, needs to be established, avoiding a fragmented approach. Any strategy for the security of information processed in an electronic form must reflect the wish of any society to operate effectively yet protect itself in a rapidly changing world.

1.2. *Objective*

A strategically orientated framework has to be established to reconcile social, economic and political objectives with technical, operational and legislative options for the Community in an international context. The sensitive balance between different concerns, objectives and constraints are to be found by sector actors working together in the development of a common perception and agreed strategy framework. These are the prerequisites for reconciling interests and needs both in policy-making and in industrial developments.

1.3. *Status and trends*

The situation is characterized by growing awareness of the need to act. However, in the absence of an initiative to coordinate efforts, it seems very likely that dispersed efforts in various sectors will create a situation which will de facto be contradictory, creating progressively more serious legal, social and economic problems.

Changes to legislation: *There are currently no known outstanding effects for the Council Decision of 31 March 1992 in the field of security of information systems (92/242/EEC). (See end of Document for details)*

1.4. *Requirements, options and priorities*

Such a shared framework would need to address and situate risk analysis and risk management concerning the vulnerability of information and related services, the alignment of laws and regulations associated with computer/telecommunications abuse and misuse, administrative infrastructures including security policies, and how these may be effectively implemented by various industries/disciplines, and social and privacy concerns (e.g. the application of identification, authentication, non-repudiation and possibly authorization schemes in a democratic environment).

Clear guidance is to be provided for the development of physical and logical architectures for secure distributed information services, standards, guidelines and definitions for assured security products and services, pilots and prototypes to establish the viability of various administrative structures, architectures and standards related to the needs of specific sectors.

Security awareness must be created in order to influence the attitude of the users towards an increased concern about security in information technology (IT).

2. Action line II — Identification of user and service provider requirements for the security of information systems

2.1. *Issue*

Security of information systems is the inherent prerequisite for the integrity and trustworthiness of business applications, intellectual property and confidentiality. This leads inevitably to a difficult balance and sometimes choices, between a commitment to free trade and a commitment to securing privacy and intellectual property. These choices and compromises need to be based on a full appreciation of requirements and the impact of possible options for the security of information systems to respond to them.

User requirements imply the security functionalities of information systems interdependent with technological, operational and regulatory aspects. Therefore, a systematic investigation of security requirements for information systems forms an essential part of the development of appropriate and effective measures.

2.2. *Objective*

Establishing the nature and characteristics of requirements of users and service providers and their relation to security measures of information systems.

2.3. *Status and trends*

Hitherto, no concerted effort has been undertaken to identify the rapidly evolving and changing requirements of the major actors for the security of information systems. Member States of the Community have identified the requirements for harmonization of national activities (especially of the ‘IT security evaluation criteria’). Uniform evaluation criteria and rules for mutual recognition of evaluation certificates are of major importance.

2.4. *Requirements, options and priorities*

As a basis for a consistent and transparent treatment of the justified needs of the sector actors, it is considered necessary to develop an agreed classification of user requirements and its relation to the provision of security in information systems.

It is also considered important to identify requirements for legislation, regulations and codes of practice in the light of an assessment of trends in service characteristics and technology, to identify alternative strategies for meeting the objectives by administrative, service, operational

***Changes to legislation:** There are currently no known outstanding effects for the Council Decision of 31 March 1992 in the field of security of information systems (92/242/EEC). (See end of Document for details)*

and technical provisions, and to assess the effectiveness, user-friendliness and costs of alternative security options and strategies for information systems for users, service providers and operators.

3. Action line III — Solutions for immediate and interim needs of users, suppliers and service providers

3.1. *Issue*

At present it is possible to protect adequately computers from unauthorized access from the outside world by 'isolation', i.e. by applying conventional organizational and physical measures. This applies also to electronic communications within a closed user group operating on a dedicated network. The situation is very different if the information is shared between user groups or exchanged via a public, or generally accessible, network. Neither the technology, terminals and services nor the related standards and procedures are generally available to provide comparable security for information systems in these cases.

3.2. *Objective*

The objective has to be to provide, at short notice, solutions which can respond to the most urgent needs of users, service providers and manufacturers. This includes the use of common IT-security evaluation criteria. These should be conceived as open towards future requirements and solutions.

3.3. *Status and trends*

Some user groups have developed techniques and procedures for their specific use responding, in particular, to the need for authentication, integrity and non-repudiation. In general, magnetic cards or smart cards are being used. Some are using more or less sophisticated cryptographic techniques. Often this implied the definition of user-group specific 'authorities'. However, it is difficult to generalize these techniques and methods to meet the needs of an open environment.

ISO is working on OSI Information System Security (ISO DIS 7498-2) and CCITT in the context of X400. It is also possible to insert security segments into the messages. Authentication, integrity and non-repudiation are being addressed as part of the messages (EDIFACT) as well as part of the X400 MHS.

At present, the Electronic Data Interchange (EDI) legal framework is still at the stage of conception. The International Chamber of Commerce has published uniform rules of conduct for the exchange of commercial data via telecommunications networks.

Several countries (e.g. Germany, France, the United Kingdom and the United States) have developed, or are developing, criteria to evaluate the trustworthiness of IT and telecommunication products and systems and the corresponding procedures for conducting evaluations. These criteria have been co-ordinated with the national manufacturers and will lead to an increasing number of reliable products and systems starting with simple products. The establishment of national organizations which will conduct evaluations and offer certificates will support this trend.

Confidentiality provision is considered by most users as less immediately important. In the future, however, this situation is likely to change as advanced communication services and, in particular, mobile services will have become all-pervasive.

3.4. *Requirements, options and priorities*

It is essential to develop as soon as possible the procedures, standards, products and tools suited to assure security both in information systems as such (computers, peripherals) and in

Changes to legislation: *There are currently no known outstanding effects for the Council Decision of 31 March 1992 in the field of security of information systems (92/242/EEC). (See end of Document for details)*

public communications networks. A high priority should be given to authentication, integrity and non-repudiation. Pilot projects should be carried out to establish the validity of the proposed solutions. Solutions to priority needs on EDI are looked at in the TEDIS programme within the more general content of this action plan.

4. Action line IV — Development of specifications, standardization, evaluation and certification in respect of the security of information systems

4.1. *Issue*

Requirements for the security of information systems are pervasive and as such common specifications and standards are crucial. The absence of agreed standards and specifications for IT security may present a major barrier to the advance of information-based processes and services throughout the economy and society. Actions are also required to accelerate the development and use of technology and standards in several related communication and computer network areas that are of critical importance to users, industry and administrations.

4.2. *Objective*

Efforts are required to provide a means of supporting and performing specific security functions in the general areas of OSI, ONP, ISDN/IBC and network management. Inherently related to standardization and specification are the techniques and approaches required for verification, including certification leading to mutual recognition. Where possible, internationally agreed solutions are to be supported. The development and use of computer systems with security functions should also be encouraged.

4.3. *Status and trends*

The United States, in particular, has taken major initiatives to address the security of information systems. In Europe the subject is treated in the context of IT and telecommunications standardization in the context of ETSI and CEN/CENELEC in preparation of CCITT and ISO work in the field.

In view of growing concern, the work in the United States is rapidly intensifying and both vendors and service providers are increasing their efforts in this area. In Europe, France, Germany and the United Kingdom have independently started similar activities, but a common effort corresponding to the United States is evolving only slowly.

4.4. *Requirements, options and priorities*

In the security of information systems there is inherently a very close relationship between regulatory, operational, administrative and technical aspects. Regulations need to be reflected in standards, and provisions for the security of information systems need to comply in a verifiable manner to the standards and regulations. In several aspects, regulations require specifications which go beyond the conventional scope of standardization, i.e. include codes of practice. Requirements for standards and codes of practice are present in all areas of security of information systems, and a distinction has to be made between the protection requirements which correspond to the security objectives and some of the technical requirements which can be entrusted to the competent European standards bodies (CEN/CENELEC/ETSI).

Specifications and standards must cover the subjects of security services of information systems (personal and enterprise authentication, non-repudiation protocols, legally acceptable electronic proof, authorization control), their communication services (image communication privacy, mobile communications voice and data privacy, data and image data-base protection, integrated services security), their communication and security management (public/private key system for open network operation, network management protection, service provider protection) and their

***Changes to legislation:** There are currently no known outstanding effects for the Council Decision of 31 March 1992 in the field of security of information systems (92/242/EEC). (See end of Document for details)*

certification (assurance criteria and levels, security assurance procedures for secure information systems).

5. Action line V — Technological and operational developments in the security of information systems

5.1. *Issue*

Systematic investigation and development of the technology to permit economically viable and operationally satisfactory solutions to a range of present and future requirements for the security of information systems is a prerequisite for the development of the services market and the competitiveness of the European economy as a whole.

Any technological developments in the security of information systems will have to include both the aspects of computer security and security of communications as most present-day systems are distributed systems, and access to such systems is through communications services.

5.2. *Objective*

Systematic investigation and development of the technology to permit economically viable and operationally satisfactory solutions to a range of present and future requirements for the security of information systems.

5.3. *Requirements, options and priorities*

Work on security of information systems would need to address development and implementation strategies, technologies, and integration and verification.

The strategic R&D work would have to cover conceptual models for secure systems (secure against compromise, unauthorized modifications and denial of service), functional requirements models, risk models and architectures for security.

The technology-orientated R&D work would have to include user and message authentication (e.g. through voice-analysis and electronic signatures), technical interfaces and protocols for encryption, access control mechanisms and implementation methods for provable secure systems.

Verification and validation of the security of the technical system and its applicability would be investigated through integration and verification projects.

In addition to the consolidation and development of security technology, a number of accompanying measures are required concerned with the creation, maintenance and consistent application of standards, and the validation and certification of IT and telecommunication products with respect to their security properties, including validation and certification of methods to design and implement systems.

The third RDT Community Framework Programme might be used to foster cooperative projects at precompetitive and prenormative levels.

6. Action line VI — Provision of security of information systems

6.1. *Issue*

Depending on the exact nature of the security features of information systems, the required functions will need to be incorporated at different parts of the information system including terminals/computers, services, network management to cryptographic devices, smart cards, public and private keys, etc. Some of these can be expected to be embedded in the hardware or software provided by vendors, while others may be part of distributed systems (e.g. network

Changes to legislation: *There are currently no known outstanding effects for the Council Decision of 31 March 1992 in the field of security of information systems (92/242/EEC). (See end of Document for details)*

management), in the possession of the individual user (e.g. smart cards) or provided from a specialized organization (e.g. public/private keys).

Most of the security products and services can be expected to be provided by vendors, service providers or operators. For specific functions, e.g. the provision of public/private keys, auditing authorization, there may be the need to identify and mandate appropriate organizations.

The same applies for certification, evaluation and verification of quality of service which are functions which need to be addressed by organizations independent of the interests of vendors, service providers or operators. These organizations could be private, governmental, or licensed by government to perform delegated functions.

6.2. *Objective*

In order to facilitate a harmonious development of the provision of security of information systems in the Community for the protection of the public and of business interests, it will be necessary to develop a consistent approach as to its provision of security. Where independent organizations will have to be mandated, their functions and conditions will need to be defined and agreed and, where required, embedded into the regulatory framework. The -objective would be to come to a clearly defined and agreed sharing of responsibilities between the different actors on a Community level as a prerequisite for mutual recognition.

6.3. *Status and trends*

At present, the provision of security of information systems is well organized only for specific areas and limited to addressing their specific needs. The organization on a European level is mostly informal, and mutual recognition of verification and certification is not yet established outside closed groups. With the growing importance of the security of information systems, the need for defining a consistent approach to the provision of security for information systems in Europe and internationally is becoming urgent.

6.4. *Requirements, options and priorities*

Because of the number of different actors concerned and the close relations to regulatory and legislative questions, it is particularly important to pre-agree on the principles which should govern the provision of the security of information systems.

In developing a consistent approach to this question, one will need to address the aspects of identification and specification of functions requiring, by their very nature, the availability of some independent organizations (or inter-working organizations). This could include functions such as the administration of a public/private key system.

In addition, it is required to identify and specify, at an early stage, the functions which in the public interest need to be entrusted to independent organizations (or interworking organizations). This could, for example, include auditing, quality assurance, verification, certification and similar functions.

Changes to legislation:
There are currently no known outstanding effects for the Council Decision of 31 March 1992 in the field of security of information systems (92/242/EEC).